Company Name:
Booz Allen Hamilton

Contract Number:
HSHQDC-06-D-00031 (HSHQDC06D00031)
HSCETC-08-J-00018 (HSCETC08J00018)

Requisition Number:
SDD-08-AF09 (SDD08AF09)

Period of Performance:
5/19/2008 through 5/18/2013

Services Provided:
This is the task order award for the Student and Exchange Visitor Information System (SEVIS), development, modernization, and enhancement.

AWARD/CONTRACT	1. THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 350)	RATING	PAGE OF PAGES 1 | 7

2. CONTRACT (Proc. Inst. Ident.) NO.	3. EFFECTIVE DATE	4. REQUISITION/PURCHASE REQUEST/PROJECT NO.
HSHQDC-06-D-00031/HSCETC-08-J-00018	05/06/2008	SDD-08-AF09

5. ISSUED BY CODE ICE/TC/IT SERVICES	6. ADMINISTERED BY (If other than Item 5) CODE ICE/TC/IT SERVIC
ICE/Info Tech Svs/IT Services Immigration and Customs Enforcement Office of Acquisition Management 425 I Street NW, Suite 2208 Washington DC 20536	ICE/Info Tech Svs/IT Services Immigration and Customs Enforcement Office of Acquisition Management 425 I Street NW, Suite 2208 Attn: Brooke Bernold Washington DC 20536

7. NAME AND ADDRESS OF CONTRACTOR (No., Street, City, Country, State and ZIP Code)	8. DELIVERY FOB ORIGIN X OTHER (See below)
BOOZ ALLEN HAMILTON INC 8283 GREENSBORO DRIVE MCLEAN VA 221023838	9. DISCOUNT FOR PROMPT PAYMENT
	10. SUBMIT INVOICES (4 copies unless otherwise specified) TO THE ADDRESS SHOWN IN ITEM
CODE 0069288570000 FACILITY CODE	

11. SHIP TO/MARK FOR CODE	12. PAYMENT WILL BE MADE BY CODE ICE-OCIO-SDD
Department of Homeland Security Immigration and Customs Enforcement Office of the Chief Info Officer 801 I Street, NW Washington DC 20536	DHS, ICE Burlington Finance Center P.O. Box 1620 Attn: ICE-OCIO-SDD Williston VT 05495-1620

13. AUTHORITY FOR USING OTHER THAN FULL AND OPEN COMPETITION:	14. ACCOUNTING AND APPROPRIATION DATA
10 U.S.C. 2304 (c) ( ) 41 U.S.C. 253 (c) ( )	See Schedule

15A. ITEM NO	15B. SUPPLIES/SERVICES	15C. QUANTITY	15D. UNIT	15E. UNIT PRICE	15F. AMOUNT
	Continued				
	15G. TOTAL AMOUNT OF CONTRACT				$6,982,345.00

16. TABLE OF CONTENTS

(X)	SEC.	DESCRIPTION	PAGE(S)	(X)	SEC.	DESCRIPTION	PAGE(S)
		PART I - THE SCHEDULE				PART II - CONTRACT CLAUSES	
	A	SOLICITATION/CONTRACT FORM			I	CONTRACT CLAUSES	
	B	SUPPLIES OR SERVICES AND PRICES/COSTS				PART III - LIST OF DOCUMENTS, EXHIBITS AND OTHER ATTACH.	
	C	DESCRIPTION/SPECS./WORK STATEMENT			J	LIST OF ATTACHMENTS	
	D	PACKAGING AND MARKING				PART IV - REPRESENTATIONS AND INSTRUCTIONS	
	E	INSPECTION AND ACCEPTANCE			K	REPRESENTATIONS, CERTIFICATIONS AND OTHER STATEMENTS OF OFFERORS	
	F	DELIVERIES OR PERFORMANCE					
	G	CONTRACT ADMINISTRATION DATA			L	INSTRS., CONDS., AND NOTICES TO OFFERORS	
	H	SPECIAL CONTRACT REQUIREMENTS			M	EVALUATION FACTORS FOR AWARD	

CONTRACTING OFFICER WILL COMPLETE ITEM 17 OR 18 AS APPLICABLE

17. X CONTRACTOR'S NEGOTIATED AGREEMENT (*Contractor is required to sign this document and return* 1 *copies to issuing office.*) Contractor agrees to furnish and deliver all items or perform all the services set forth or otherwise identified above and on any continuation sheets for the consideration stated herein. The rights and obligations of the parties to this contract shall be subject to and governed by the following documents: (a) this award/contract, (b) the solicitation, if any, and (c) such provisions, representations, certifications, and specifications, as are attached or incorporated by reference herein. *(Attachments are listed herein.)*

18. AWARD (*Contractor is not required to sign this document.*) Your offer on Solicitation Number HSCETC-08-Q-00007, including the additions or changes made by you which additions or changes are set forth in full above, is hereby accepted as to the items listed above and on any condition sheets. This award consummates the contract which consists of the following documents: (a) the Government's solicitation and your offer, and (b) this award/contract. No further contractual document is necessary.

19A. NAME AND TITLE OF SIGNER (Type or print)	20A. NAME OF CONTRACTING OFFICER
Ronald A. Hodge, Vice President	JoNelle M. Hildreth

19B. NAME OF CONTRACTOR	19C. DATE SIGNED	20B. UNITED STATES OF AMERICA	20C. DATE SIGNED
BY (b)(4) *(Signature of person authorized to sign)*	05/06/08	BY *(Signature of the Contracting Officer)*	

NSN 7540-01-152-8069
PREVIOUS EDITION IS UNUSABLE

STANDARD FORM 26 (Rev. 4-85)
Prescribed by GSA
FAR (48 CFR) 53.214(a)

NAME OF OFFEROR OR CONTRACTOR

BOOZ ALLEN HAMILTON INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	DUNS Number: 006928857 The following is the Task Order award for the Student and Exchange Visitor Information System, Development, Modernization, and Enhancement, HSCETC-08-J-00018, under Booz Allen Hamilton's EAGLE Contract HSHQDC-06-D-00031. FOB: Destination Period of Performance: 05/19/2008 to 05/18/2013				
0001	Configuration Management Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: (b)(2)High Funded: (b)(4)	1	LO	(b)(4)	
0001A	Configuration Management (Option Line Item) 05/19/2009 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
0002	Software Development Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: (b)(2)High Funded: (b)(4)				(b)(4)
0002A	Software Development (Option Line Item) 05/19/2009 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Continued ...				0.00

NAME OF OFFEROR OR CONTRACTOR

BOOZ ALLEN HAMILTON INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Accounting Info: Funded: $0.00				
0003	Data Migration and Transition Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: (b)(2)High Funded: (b)(4)				(b)(4)
0003A	Data Migration and Transition (Option Line Item) 05/19/2009 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
0005	Manage System Change Requirements Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00	1	LO	0.00	0.00
0005A	Manage System Change Requirements (Option Line Item) 05/19/2009 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
0006	Training Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Continued ...				(b)(4)

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	(b)(2)High Funded: (b)(2)High				
0006A	Training (Option Line Item) 05/19/2009 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
1001	Configuration Management (Option Line Item) 05/19/2010 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
1002	Software Development (Option Line Item) 05/19/2010 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
1004	Operations and Maintenance Support (Option Line Item) 05/19/2010 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
1005	Manage System Change Requirements (Option Line Item) 05/19/2010 Product/Service Code: R425 Continued ...				0.00

NAME OF OFFEROR OR CONTRACTOR

BOOZ ALLEN HAMILTON INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				
1006	Training (Option Line Item) 05/19/2010 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
2001	Configuration Management (Option Line Item) 05/19/2011 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
2002	Software Development (Option Line Item) 05/19/2011 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
2004	Operations and Maintenance Support (Option Line Item) 05/19/2011 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
2005	Manage System Change Requirements (Option Line Item) 05/19/2011 Product/Service Code: R425 Continued ...				0.00

NAME OF OFFEROR OR CONTRACTOR

BOOZ ALLEN HAMILTON INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				
2006	Training (Option Line Item) 05/19/2011 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
3001	Configuration Management (Option Line Item) 05/19/2012 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
3002	Software Development (Option Line Item) 05/19/2012 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
3004	Operations and Maintenance Support (Option Line Item) 05/19/2012 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				0.00
3005	Manage System Change Requirements (Option Line Item) 05/19/2012 Product/Service Code: R425 Continued ...				0.00

NAME OF OFFEROR OR CONTRACTOR

BOOZ ALLEN HAMILTON INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00				
3006	Training (Option Line Item) 05/19/2012 Product/Service Code: R425 Product/Service Description: ENGINEERING & TECHNICAL SERVICES Accounting Info: Funded: $0.00 Administrative Contracting Officer: Brooke Bernold, (b)(6) 202-616-(b)(6) The total amount of award: $30,531,043.00. The obligation for this award is shown in box 15G.				0.00

~~**PROCUREMENT SENSITIVE See FAR 3.104**~~

U.S. Department of Homeland Security (DHS)
Immigration and Customs Enforcement (ICE)

Student Exchange Visitors Program (SEVP)
&
Office of the Chief Information Officer (OCIO)

Statement of Work

Version 1

Development, Modernization, and Enhancement (DME) with Follow-on Operations and Maintenance (O&M) Services
for

Student and Exchange Visitor Information System (SEVIS II)

Office of the Chief Information Officer
801 I Street, N.W.
Washington, D.C. 20536

December 7, 2007 Original Release
January 25, 2008 Revised Section 9.0
May 1, 2008 Replaced Section 15.0

TABLE OF CONTENTS

1.0 Project Title

Student and Exchange Visitor Information System II (SEVIS II).

2.0 Background

SEVIS is an Internet-based information system for non-immigrant foreign students (F Visa for academic students and M Visa for vocational students), exchange visitors (J Visa), their dependents (F-2, M-2, and J-2), and the schools and program sponsors approved to access SEVIS and host non-immigrants. In short, SEVIS enables schools and program sponsors to transmit electronic information and event notifications, via the Internet, to the Department of Homeland Security (DHS) and the Department of State (DOS) throughout a student's or exchange visitor's stay in the United States.

The Immigration and Customs Enforcement (ICE) seeks to replace the current system (SEVIS I) with an updated system based on a completely different architecture. We take this initiative for two compelling reasons. First, SEVIS I does not adequately meet the needs of the national security, law enforcement, and academic communities, all of whom rely heavily on SEVIS I data and its interoperability. Second, a February 5, 2007 review by the Border and Transportation Policy Coordination Committee (PCC), under the direction and authorization of the Homeland Security Council (HSC), identified several serious national security vulnerabilities inherent in SEVIS I. Additionally, the PCC made several recommendations to close those vulnerabilities.

SEVIS I shortcomings stem primarily from the fact that it was designed to track documents instead of individuals, thus creating the real possibility of an individual being identified by numerous different records within the system and making it almost impossible to comprehensively track all of the activities of an individual. SEVIS I originated as an immigration benefits tracking tool. Throughout its short existence, thousands of changes and revisions have been made to SEVIS I to adapt it to the ever-growing needs of its users. Despite all of these often costly changes, SEVIS I still faces significant limitations.

Today, SEVIS I is utilized as a critical national security database. It is regarded as a primary resource for conducting threat analysis for counterterrorism and/or counterintelligence by the law enforcement and intelligence communities; key attributes which were not initially developed into the SEVIS I deliverable. Two primary law enforcement/intelligence users of SEVIS I are the Foreign Terrorist Tracking Task Force (FTTTF) and the ICE Compliance Enforcement Unit (CEU).

A comprehensive SEVIS I feasibility study completed by ICE in January 2007 determined that no amount of costly and substantial changes to SEVIS I could address the many improvements strongly sought by the academic, law enforcement, and national security communities.

Thus, the objective of SEVIS II is to close the PCC-identified vulnerabilities and meet the growing needs of all stakeholder communities by maintaining pace with today's emerging law enforcement technologies. SEVIS II will provide hundreds of significant enhancements in five major areas:

- Convert from a largely paper-based, manual system to a real-time, automated system with electronic forms (e-forms);
- Greatly enhanced ability to search the system (without running ad hoc reports), increased efficiency, and decreased risk of user error;
- Use the Fingerprint Identification Number (FIN) as a biometric identifier to accurately and rapidly match records to their owners (one person – one record);
- Utilizing the current DHS enterprise architecture (EA) structure, create a system that integrates well with existing systems and is open, flexible and scalable (Interoperability with other US Government agency systems will provide critical real-time national security information) and;
- Greatly enhance Domestic Mantis – Enhancement of the system to track and provide reports that are indicative of 'changes of academic majors' and 'identification of designated academic courses that are of national security interest.

These improvements will serve to close data vulnerabilities, as well as reduce the margin for error or abuse of the system by potential students and visitors to our country. SEVIS II will be the main repository of record, providing updated, correct and expedient/real-time information to law enforcement and academic users/stakeholders.

3.0 Scope of Work

The contractor shall perform work under this SOW as it pertains to the EAGLE contract functional category 4 - Software Development.

The specific objective of the proposed task order is to provide technical services for design, development, implementation and maintenance of SEVIS II. SEVIS II will be designed to integrate with existing DHS systems; such as Password Issuance Control System (PICS), Computer-Linked Application Information Management System (CLAIMS) Interface, DoS Consulate, Arrival/Departure Information System (ADIS), Non-Immigrant Visa Interface (NIV), I-901 Fee Pay, U.S. VISIT (SEVIS sends specific records in support of U.S. VISIT), Foreign Terrorist Task Tracking Force (FTTTF), and USCIS Verification Information System (VIS). Additionally, SEVIS II will be enhanced to also interface with I-17 (within Pay.Gov), NSEERS and IBIS (CBP systems), and the Alien Flight Student Program (AFSP) (a Transportation Security Administration (TSA) system). The system functionality will also be in accordance with DHS Strategic Plan goals of Awareness and Prevention.

SEVIS II consists of e-Gov Internet, ICE intranet, and Tier 1/2/3 Help Desk functionalities that require technical support. The web based platforms are currently located in Rockville, MD at the Department of Justice (DOJ) Data Center, with an anticipated move in the future to the Department of Homeland Security (DHS) Data Center in Stennis, MS. The Tier 1 Help Desk is currently located at a contractor facility in Colorado Springs, CO. ICE requires all functionality to be maintained (operational) on a 24 x 7 day basis. Each area has specific system and personnel requirements, which are provided in detail as a part of the solicitation package.

The contractor shall ensure that software developed under the contract maintains a level of scalability for additional non-immigrant categories as determined by future congressional and

DHS mandates and regulatory directives. Additionally, the contractor shall be required to incorporate future iterations of flight school training/programs via single or multiple interfaces. VISA categories will be determined by DHS as mandates are imposed.

4.0 Applicable Documents

4.1 Technical Documents

The technical documents below are applicable to this SOW and can be made available as part of Government Furnished Information (GFI):

- ICE Technical Architecture Guidebook
- ICE Enterprise Systems Assurance Plan
- ICE Architecture Test and Evaluation Plan
- ICE Web Standards and Guidelines
- ICE System Lifecycle Management (SLM) Manual
- DHS EAGLE Ordering Guide
- ICE Approved Software List

4.2 Other Supporting Documentation and Guidance

The documents listed below can be made available as part of Government Furnished Information (GFI).

- DHS/ICE Baseline Security Requirements for Automated Information Systems, July 18, 2003.
- ICE Security Requirements, printed October 30, 2003.
- IT Security Program Handbook, Version 1.3, Sensitive Systems, Department of Homeland Security, ID-4300A, June 20, 2003.

5.0 Specific Tasks

5.1 Performance Standards

The Contractor shall comply with all technology standards and architecture policies, processes, and procedures defined in ICE OCIO Architecture Division publications. These publications include, but are not limited to, the following:

- ICE Technical Architecture Guidebook
- ICE Systems Lifecycle Management (SLM) Manual
- ICE Enterprise Systems Assurance Plan
- ICE Architecture Test and Evaluation Plan and
- ICE Web Standards and Guidelines

The Contractor shall not deviate from the Technology Standards without approval granted by the Government via the formal Technology Change Process. If a deviation from the Technology Standards is desired, the Government Project Manager must submit a formal request to the Architecture Division for adjudication. The Contractor may not proceed with the deviation

unless Architecture Division approves the formal request and grants a waiver to deviate from the Technology Standards. If Architecture Division approves the technology change request, the Contractor shall comply with all stipulations specified within the approval notification.

The Contractor shall not deviate from the SLM Process (including a Tailored SLM work pattern) without express approval granted by the Government Program Manager(s) via the formal Request for Deviation (RFD) Process. If a deviation from the SLM Process is desired, the Government Project Manager must submit a formal FRD to Architecture Division for adjudication. The Contractor may not proceed with the deviation unless Architecture Division approves the formal request and grants a waiver to deviate from the SLM Process. If Architecture Division approves the FRD, the Contractor shall comply with all stipulations specified within the approval notification.

Prior to start of a system modification, the contractor and the Government Program Manager(s) shall agree on the extent of all work to be performed. The Contracting Officer and COTR must approve System Change Requests (SCRs) for which the estimate to complete exceeds the 500 hour maximum. The contractor shall update Tracker to reflect SCR disposition. The contractor shall be responsible for carrying out all maintenance for SEVIS according to open SCRs identified in the Tracker.

The contractor shall manage and maintain SEVIS II to identify and correct software failures, performance failures, and implementation failures for all SEVIS II components. SEVIS II maintenance includes emergency repairs performed when immediate correction is necessary to continue user service; corrective work includes SCRs performed to reflect the requirements/specifications; and, updating and maintaining the required SLM documentation as necessary.

The contractor shall assess and maximize the reuse potential of current SEVIS functionality and technology for use in SEVIS II. The contractor is required to provide an initial report detailing their architectural approach, implementation strategy, and their ability to reinforce other ICE mission applications.

5.2 Configuration Management:

The contractor shall conduct configuration management for all development and maintenance tasks under the guidelines set forth by the ICE OCIO Architecture Division; conduct project-level configuration management for all development and maintenance work for the applications/database; execute all approved requests for changes to establish baselines via the approved SCR process, including the chartering and conducting Change Control Board (CCB) meetings; assign proper identification of all configuration items in accordance with agreed on conventions. This includes the proper labeling of all software releases, regardless of content; and, submits an electronic version of all deliverables to the Electronic Library Management System (ELMS) library.

5.3 Software Development

The contract shall develop software in compliance with Capability Maturity Model Integration (CMMI) Level 2 standards.

The Contractor shall:

- Develop a system that provides a level of scalability and compatibility with other DHS and DOS systems and is always in compliance with emerging DHS enterprise architecture. This includes biometrics via the US-VISIT IDENT FIN biometric services. Outside users such as universities must be able to access the system; therefore, these users should be consulted during the requirements and development phases. Additionally, the contractor shall develop an account set-up capability in the absence of a DHS enterprise solution that can be extended or reused to support the USCIS Transformation Program requirements.
- Develop a system that will focus on the "one person, one record" principle. The system should recognize the person each time they are entering the U.S. based on a biometric identification process.
- Develop software that will allow users to view historical data for each individual. Authorized users include, but not exclusively, employees and staff of the SEVP; authorized enforcement agents nationwide; and, Department of State Consulate users. The software design should allow for expanding the number of authorized users.
- Develop software that will allow for broader search/query capabilities, avoiding and/or eliminating the need to continually require ad hoc code writing. Based on user input, the contractor should be amenable to tailoring the software to fit the needs and circumstances of the user, consistent with his or her authorization level. They must incorporate Soundex-type and/or "fuzzy" search capacities for names and should permit queries based on date ranges and other available data fields.
- Develop software that shall enhance the I-17 school certification module to have the same functionality/capabilities as the I-17 Tracking and Reporting System (ITARS). ITARS is a custom created software package. The enhancement of the I-17 school certification module to do everything that the ITARS standalone currently does will eliminate the necessity of that system. Concurrently, the I-17 module should be revised to take into account the field inspection activity that underpins every school certification. Contract field inspectors and their managers should be given access into the revised I-17 portal to permit field inspections to be entered and completed online.
- Develop software that will allow for a stronger/broader electronic link between the SEVIS II, Pay.Gov and the I-901 Fee Module. Incorporating stronger electronic links between SEVIS II and Pay.Gov and the I-901 fees module should include permitting enforcement users to view the fee payment data associated with the applicant.
- Develop software that allows for most of the processes and forms to be "paperless." This development should include designing the I-20 and its exchange program parallel, the DS-2019, as "virtual" forms.
- Develop software that will incorporate input masks that will preclude inappropriate data entry of key fields (such as "UNK" in name fields). Also, this software shall be able to force compliance with standard entry procedures for other key fields (such as social security numbers, telephone numbers, dates, and A-numbers) and require users to enter certain fields (such as email addresses) and confirm/verify (with an additional entry) their choices**.** This

would eliminate many data integrity problems and minimize re-work for staff such as the Help Desk.

- Develop and implement interactive training sessions for new front-end users at schools, and exchange programs**.** The training should be accessed directly from SEVIS II, as opposed to a separate website. A yearly refresher course will also be required.
- If approved by ICE management, incorporate an automatic suspension of users if their data error rates exceed a certain threshold (to be set at a later date).
- Design and implement a background check and certification process for P/DSOs Principal Designated School Officials (PSOs)/Designated School Officials (DSOs) and Alternate Responsible Officers (AROs)**.**
- Design the software with internal flagging capability based on NSEERS-designated categories**.** These flags would permit prioritizing leads to be pursued by the CEU or other enforcement entities.

5.4 Data Migration and Transition

Data from the various legacy systems contributing to an integrated solution will be converted to a normalized and consistent form, and loaded into a common database. Data conversion shall be accomplished with automated routines as much as possible. Further, to the extent imposed by the available legacy data, manual procedures and processes will be developed and executed to support efficient transformation of existing data into the consistent, normalized form required by a common database. The contractor will be required to work with the incumbent contractor for data migration.

5.5 Operations and Maintenance (O&M)

The contractor shall fully maintain the SEVIS II application system and software developed under this task and application software. Tasks include, but are not limited to the following tasks:

- Maintain the application to identify and correct software application and performance failures, and implementation failures for all SEVIS II components. Maintenance includes emergency repairs performed when immediate correction is necessary to continue user service; corrective work [includes System Change Requests (SCRs)] performed to reflect the requirements/specifications; and, updating and maintaining the required SLM documentation as necessary.
- Perform maintenance tasks to meet changes in requirements of the users or user environment; enhance the system to provide additional or changed functionality; adapt the system to changes in business processes; or extend software to new users.
- Maintain the current external SEVIS II interfaces as identified.
- Provide coordination with HQICE and field personnel, including assistance with getting potential users into SEVIS II, and preparation of information to be disseminated to customers, including brochures and informational sheets.
- Provide updated Standard Operating Procedures (SOPs), scripts and procedures to Tier 2 Help Desk staff when new information, releases or changes regarding SEVIS II have been distributed and/or implemented.

- Meet with the HQICE Program and Policy personnel on the technical issues on a weekly or as needed basis.
- Meet with the HQ OCIO Program and Policy personnel on the technical issues on a weekly or as needed basis.
- Perform all system administration activities associated with ICE application processes under this SOW, as specified. These activities shall include monitoring and compilation of data statistics for batch and interface production processing; identification of corrupt files or processes; and system archiving and data archiving when applicable.
- Provide Help Desk Support. The help desk requirements include the following:
  - Provide Tier 1 support that consists of receiving initial requests for service, providing telephone assistance in resolving the reported problem, tracking the request from receipt of call to completion of service or escalating calls to the next level as required and issuing customer surveys.
  - Personnel will accomplish the task with the following minimum qualifications as required by the position:
    - Experience in working on multiple projects simultaneously in a Help Desk environment
    - Experience dealing with a variety of people from varying professional/administrative backgrounds.
    - Demonstrated ability to communicate effectively both orally (in groups and one-on-one) and in writing (dictated by position occupied).
    - Demonstrated ability to work independently and as a team leader (dictated by position occupied).
    - Demonstrated ability to efficiently interpret and analyze information from various sources.
  - If changes in staff are necessary, replacements shall be as qualified as the predecessors. Resumes of proposed replacements shall be provided at least two-weeks in advance of the proposed change to allow a reasonable amount of time to review the proposed change.
- Be responsible for the actions and daily supervision of its employees while on government property. All contractor personnel shall present a clean and professional appearance. On-site, contractor "office" personnel shall wear appropriate business attire the same as that normally worn by professional or executive government personnel. The contractor shall display the ICE-issued identification badge at all times.
- Provide on-site support from 8:00 a.m. to 8:00 p.m. (EST/EDT) Monday through Friday (except for Federal Holidays). There will be no overtime unless there is an emergency request authorized by the COTR.
- Provide full-time, experienced Help Desk Specialists to operate a national SEVIS II Help Desk consisting of capabilities that include the operation of Remedy software for recording and tracking all trouble reports;
- Provide Tier 2 Help Desk Support. This support includes:
  - Specific questions/problems related that Tier 1 is unable to resolve. Issues that must be coordinated with technicians;

- Specific requests that must be coordinated with database administrators to perform data fixes to records.
- Compile statistical, workload, and trend analysis reports, including the continuation of the current daily Excel reports from the database containing batch statistics, etc; and,
- Provide updated Standard Operating Procedures (SOPs), scripts and procedures to Tier 2 Help Desk staff when new information, releases or changes regarding SEVIS II have been distributed and/or implemented.
- Conduct Tier 1 and Tier 2 Help Desk weekly meetings together to ensure coordination and information dissemination; and conduct weekly meetings with the Tier 1 national help desk for coordination and information dissemination.

5.6 Manage System Change Requirements

Software changes to applications are based upon the submission and government approval of a System Change Request (SCR). The contractor shall be responsible for carrying out all application maintenance requirements projects according to open SCRs and entering the data in the ICE approved management tracking tool. Currently ICE uses Serena Tracker. Prior to commencing a system modification, the contractor and the OCIO Project Manager shall agree on the degree of the modification as minor, moderate or major. (See table below for classification).

Change Classification	Estimated Effort Required
Minor Change	1 – 40 Hours
Moderate Change	41 – 160 Hours
Major Change	160 – 500 Hours

Emergency maintenance will be performed at the direction of the government. The respective OCIO Project Manager must approve all SCRs in writing.

The following requirements apply to each of the tasks:

- Performance Standards – All software maintenance is to be performed in accordance with (IAW) the ICE SLM procedures.
- Deliverables – Products and updated SLM documentation as required; ad hoc reports; SCRs created for problem reports and entered into Tracker.

5.7 Training

The Contractor shall support application implementation and deployment through technical and end-user training whenever changes to the application are significant enough to warrant such training. Specifically, the contractor shall:

- Maintain and update existing technical and end-user training documentation. They shall also provide an electronic copy of all training material whenever an update is developed;
- Develop and conduct one-on-one and train-the-trainer type training classes when major releases/additions to documentation have occurred; and,

- Provide training on how to use SEVIS II for Immigration Inspectors located at the Ports of Entry, the Compliance Enforcement Unit, Analysts at the Federal Bureau of Investigation (FBI), DSO, RO, DHS and other authorized agency personnel approved by the COTR.

5.8 Optional Tasks

The first two tasks involve the use of emerging DHS enterprise solutions, whose requirements are still in the planning phase. The third task involves an interface between SEVIS II and the Transportation Security Administration (TSA) Alien Flight Student Program (AFSP)

5.8.1 Optional Task 1

The contractor will be required to modify the proposed solution in order to align with the DHS Portal Standards. At the release of this SOW, the DHS Portal Standards were still under internal review. Once finalized, the standards will be delivered to the contractor for review. The contractor is required to provide DHS with a work breakdown structure and cost estimate for the work required.

5.8.2 Optional Task 2

The contractor will be required to modify the proposed solution to incorporate the DHS E-Authentication solution into the overall architecture of SEVIS II. At the release of this SOW, the details and specifications of the DHS E-Authentication solution were still under internal review. Once finalized, these specifications will be delivered to the contractor for review. The contractor is required to provide DHS with a work breakdown structure and cost estimate for the work required.

5.8.3 Optional Task 3

The contractor will be required to modify the proposed solution to incorporate and interface with the AFSP. At the release of this SOW, the requirements surrounding an interface with the AFSP were still under internal review. Once finalized, these requirements will be delivered to the contractor for review. The contractor is required to provide DHS with a work breakdown structure and cost estimate for the work required.

6.0 Key Personnel

The Government has determined that the Project Manager and Project Leads are key personnel for this Scope of Work. The Contractor may designate other positions as necessary as key to the work to be performed under this contract.

The Project Manager shall possess the technical and leadership skills requirements set forth under the labor categories in the DHS EAGLE contract. In addition to those skills, it is desired

that the Project Manager also possess a Master's degree, be PMP certified, and have 8-10 years of IT-related program management experience or have experience managing law enforcement, biometric-capable and/or enterprise-wide systems.

Project Leads shall possess the skills and abilities as stipulated in the DHS EAGLE contract. In addition to those skills, it is desired that the proposed Project Leads possess a Bachelor's degree, 5-7 years of IT-related management experience or have experience managing law enforcement, biometric-capable, and/or enterprise-wide systems.

7.0 Deliverables and Delivery Schedule

All deliverables shall be delivered to the Federal Protective Service/Student Exchange Visitor Program Branch (FPS-SEVP), ICE OCIO; Room 620; 801 I Street NW; Washington, DC; 20536 not later than 3:00 PM on the deliverable's due date. Specific deliverables related to each activity are outlined in below:

Deliverables Summary and Metrics

Deliverable	Frequency	Copies	Recipients
Software Versions and Releases	As Required	2 CDs 1 PC	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
Financial Reports (EVMS, Invoices and Funds Status)	Monthly	2 CDs 1PC	TM (2) copy/ COTR (1) copy / CO (trans ltr.)
SLM Documentation	As Required	2 CDs 1 PC	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
Project Plans/Schedules	As Required	2 CDs 1 PC	TM (3) copy/ COTR (trans ltr.), CO (trans ltr.)
Progress Reports	Monthly	2 CDs 1 PC	TM (2) copy/ COTR (1) copy/ CO (trans ltr.)
Quality Assurance Reports	Quarterly	2 CDs 1 PC	TM (2) copy/ COTR (1) copy/ CO (trans ltr)

Task Manager will receive one (1) CD and one (1) printed paper copy of each deliverable.

7.1 Project Plan and Schedule

The contractor shall develop a Project Plan, outlining resources, activities, and milestones necessary to accomplish work specified in the SOW. Technical activities in the schedule shall be at a level of detail sufficient for the contractor to manage the task. The contractor shall develop a

new Project Plan schedule whenever a modification to the contract occurs. The contractor shall provide the initial plan within thirty (30) days of award.

The contractor shall schedule activities specified in the SOW including:

- Management activities
- Product Assurance activities
- Design activities
- Development activities
- Test activities
- Deployment activities (each site)
- Operations and Maintenance activities
- Reviews
- Releases
- Milestones
- Decision points

The contractor shall provide an initial schedule and monthly update for each Contract Line Item Numbers (CLINs) to the COTR.

7.2 Progress Reports, Status Reports & Program Reviews

7.2.1 Progress Reports

The contractor shall prepare a monthly progress report. Initial reports are due to the COTR 30 days after award and every 30 days thereafter until the last month of performance; the final delivery will occur ten (10) days before the end of the final option period and will summarize performance during the period of performance and provide the status of any planned transition activity. The monthly report shall contain the following:

- Description of work planned
- Description of work accomplished
- Analysis of the difference between planned and accomplished
- Work planned for the following month
- Open issues

7.2.2 Quarterly Status Report

The contractor shall prepare a quarterly status report for the CO and the COTR. Generally, these reports should include accomplishments, any deviations from planned activities, field related issues, other issues, and planned activities for the next period. The reports are for the CO and COTR, and may be delivered in hardcopy or via electronic (e-mail). Additionally, the CO and/or the COTR may request impromptu meetings to discuss status or issues.

7.2.3 Program Reviews

The contractor shall participate in quarterly Program Reviews with the COTR or designee to review selected projects. The purpose of this meeting is to ensure the state of production processing; and, that all application software efforts are coordinated, consistent, and not duplicative. Budgets, schedules and other program related issues shall also be addressed when required. The program review is intended to be an informal executive summary of these events, and should require only minimal presentation time.

7.2.4 Project Plan and Schedule Deliverables

For all Project Plans and Schedules, the contractor shall deliver two (2) copies of each deliverable to the ICE task manager, one (1) on CD and one (1) hard copy format; one (1) copy of the letter of transmittal without attachments shall be delivered to the COTR and the contracting officer.

7.3 Cost/Schedule & Earned Value Management System (EVMS) Report

The contractor shall submit monthly reports to the COTR. The reports must be prepared in sufficient detail to support OMB A-11 reporting requirements at Exhibits 53 and 300. The initial report is due 45 calendar days after Contract award and shall cover the first 30 days of Contract performance. Subsequent reports will be provided monthly and shall cover the 30-day period that began at the conclusion of the last reported period.

DHS requires use of EVM on all major investments (Level 1, Level 2, and IT Level 3) in development with a total acquisition cost of $20 mil and greater and on major systems in development and on their associated contracts with a contract price at $20 mil and greater. SEVIS II has been classified as a Level 1 investment.

7.4 Financial Reporting

The Contractor shall submit monthly reports to the ICE's COTR that must be prepared in sufficient detail to support OMB A-11 reporting requirements at Exhibits 53 and 300. The initial report is due forty-five calendar days after award and shall cover the first thirty days of performance. Subsequent reports will be provided monthly and shall cover the thirty-day period that began at the conclusion of the last reported period. The Contractor shall provide the required reports in accordance with the format provided by the COTR.

The contractor shall prepare a monthly Excel workbook containing one sheet per task and a summary sheet. The Contractor shall provide the following information on each sheet:

- Cost Ceiling, Proposal Burn rate, Proposal Cumulative, Funding Ceiling
- Monthly Incurred, Cumulative Incurred
- Monthly Outlook, Total Estimated Cost
- Monthly Invoiced, Cumulative Invoiced

Monthly and summary data shall be provided for the above information. An imbedded chart shall also be included on the sheet with a primary axis containing the monthly incurred and the monthly outlook; and a secondary axis containing the remaining information.

The contractor shall deliver one (1) CD copy and one (1) paper copy to the TM, one (1) CD copy to the COTR with a letter of transmittal; one (1) copy of the transmittal letter will be addressed to the contracting officer without attachments.

7.5. SLM Deliverables

For all SLM deliverables, the contractor shall deliver one (1) CD copy and one (1) paper copy to the TM, one (1) CD copy to the COTR with a letter of transmittal; one (1) copy of the letter of transmittal without attachments shall be delivered to the contracting officer.

7.6 Quality Assurance Reports

The contractor shall deliver Quality Assurance Reports as follows: one (1) CD copy and one (1) paper copy to the TM, one (1) CD copy to the COTR with a letter of transmittal; and a letter of transmittal without attachment will be provided to the contracting officer.

7.7 Ad Hoc Deliverables

All other Contract deliverables shall be delivered in accordance with instructions specified at the relevant sections of the SOW.

7.8 Product Acceptance

Information technology products delivered under this SOW shall be accepted when they meet all requirements, which include: validating objectives, processes and functionality, technical accuracy or merit, compliance to ICE technical standards, and all Coordination, Review and Approval Forms required by the SLM Manual are completed.

Initial deliverables shall be considered draft versions and will be reviewed and accepted or rejected by the government within ten working days. The documents shall be considered final upon receiving government approval.

8.0 Government Furnished Equipment and Information

A CD with all available documentation relevant to SEVIS II will be provided to the contractor upon release of the SOW. Upon award (and obtaining required security clearance); the contractor will be provided access to the Enterprise Library located at 1101 Vermont Avenue, NW, Suite 220, Washington, DC, 20005. The Enterprise Library is the central repository for all ICE IT Systems documentation.

9.0 Place of Performance

During the development and testing of SEVIS II and when on-going O & M support is being provided; work, meetings and briefings will be performed primarily at contractor's facilities or at the government's option at ICE offices in the Washington, DC. Frequent travel to ICE OCIO offices located at 801 I Street NW, Washington DC, 20536 may be required. The contractor's facility shall be within 30 minutes travel time to the ICE OCIO offices. Normal operations must be carried on during on during an 8 hour period between the hours of 8:00 am and 6:00 pm, Monday through Friday except federal holidays, unless otherwise authorized by the ICE Task Manager.

The place of performance for the Help Desk, Tiers 1 and 2, will be at the discretion of the contractor.

Travel to sites outside of the Washington, DC area if required in conjunction with the performance of Contract project requirements will be in accordance with the Joint Travel Policy shall be adhered to by the contractor. Advanced notice and approval must be provided for any travel required.

10.0 Period of Performance

SEVIS II requirement will consist of a two-year base period and three one-year option periods for the FC 4. The base period will begin upon award.

Base Period (2 years)	Upon Award	For 24 months
Option Period 1	End of Base Period	For 12 months
Option Period 2	End of Option Period 1	For 12 months
Option Period 3	End of Option Period 2	For 12 months

11.0 Security

A) General Clause
To ensure the security of the DHS/ICE information in their charge, ICE contractors and sub-contractors must adhere to the same computer security requirements and regulations as ICE federal employees unless an exception to policy is agreed to by the prime contractors, ICE ISSM and Contracting Officer and detailed in the contract. The DHS Rules of Behavior document apply to both DHS federal employees and DHS support contractors and sub-contractors.

B) Security Policy References Clause
The following three primary DHS/ICE IT Security requirements documents are applicable to contractor/subcontractor operations supporting Sensitive But Unclassified (SBU) based contracts. Additionally, ICE and its contractors must conform to other DHS Management Directives (MD) (Note: these additional MD documents appear on DHS-Online in the Management Directives Section. Volume 11000 "Security and Volume 4000 "IT Systems" are of particular importance in the support of computer security practices)

- DHS 4300A Sensitive Systems Policy Directive (ICE OISS Intranet Site)
- DHS 4300A, IT Security Sensitive Systems Handbook (ICE OISS Intranet Site)
- ICE Directive, IT Security Policy Supplemental for SBU Systems (ICE OISS Intranet Site)

C) Contractor Information Systems Security Officer (ISSO) Point of Contact Clause
The Contractor must appoint and submit name to ICE Information Systems Security Manager (ISSM) for approval, via the ICE COTR, of a qualified individual to act as ISSO to interact with ICE personnel on any contractor IT security issues.

D) Protection of ICE Sensitive But Unclassified Information
The Contractor shall protect all DHS/ICE "sensitive information" to which the Contractor is granted physical or electronic access by adhering to the specific IT security requirements of this contract and the DHS/ICE security policies specified in the Reference Section above. Contractor shall ensure that their systems containing DHS/ICE information and data be protected from unauthorized access, modification and denial of service. Further, the data must be protected in order to ensure the privacy of individual's personal information.

12.0 Other Direct Costs (ODCs)

The government does not foresee substantial requirements for recurring ODC expenditures for travel, training, or equipment against this contract. However, the contractor shall propose all other anticipated ODC necessary to comply with the requirements of this Contract with appropriate justification and explanation in its technical and cost proposals. Once accepted, proposed ODC will be considered part of the total estimated cost of performance. Each travel, training, or equipment ODC expenditure shall be pre-approved by the COTR in accordance with the following guidance:

Travel outside the local metropolitan Washington, DC area may be expected during performance of the resulting contract. Therefore, travel will be undertaken following the General Services Administration Joint Travel Regulation. Reimbursement for allowable costs will be made.

13.0 Accessibility Requirements

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

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

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

36 CFR 1194.23 – Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.

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. This standard applies to any training videos provided under this work statement.

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

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

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

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

14.0 Security Requirements

Security Requirements for Unclassified Information Technology Resources (June 2006)

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

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

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

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 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.

15.0 Contractor Personnel Security Requirements

A) General

The Department of Homeland Security (DHS) has determined that performance of the SEVIS II DME tasks requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor) have access to sensitive DHS information, and that the Contractor will adhere to the following.

B) Suitability Determination

DHS shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the contract. No employee of the Contractor shall be allowed to EOD and/or access sensitive information or systems without a favorable EOD decision or suitability determination by the Office of Professional Responsibility, Personnel Security Unit (OPR-PSU). No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the OPR-PSU. Contract employees assigned to the contract not needing access

to sensitive DHS information or recurring access to DHS ' facilities will not be subject to security suitability screening.

C) Background Investigations

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. Background investigations will be processed through the Personnel Security Unit. Prospective Contractor employees with adequate security clearances issued by the Defense Industrial Security Clearance Office (DISCO) may not be required to submit complete security packages, as the clearance issued by DISCO may be accepted. Prospective Contractor employees without adequate security clearances issued by DISCO shall submit the following completed forms to the Personnel Security Unit through the COTR, no less than 5 days before the starting date of the contract or 5 days prior to the expected entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions" Form will be submitted via e-QIP (electronic Questionnaires for Investigation Processing) **(2 copies)**

2. FD Form 258, "Fingerprint Card" **(2 copies)**

3. Foreign National Relatives or Associates Statement

4. DHS 11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"

5. Optional Form 306 Declaration for Federal Employment (applies to contractors as well)

6. Authorization for Release of Medical Information

Required forms will be provided by DHS at the time of award of the contract. Only complete packages will be accepted by the OPR-PSU. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive information has resided in the US for three of the past five years, the Government may not be able to complete a satisfactory background investigation. In such cases, DHS retains the right to deem an applicant as ineligible due to insufficient background information.

The use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), is not permitted in the performance of this contract for any position that involves access to, development of, or maintenance to any DHS IT system.

D) Continued Eligibility

If a prospective employee is found to be ineligible for access to Government facilities or information, the COTR will advise the Contractor that the employee shall not continue to work or to be assigned to work under the contract.

The OPR-PSU may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

The OPR-PSU may require reinvestigations when derogatory information is received and/or every 5 years.

DHS reserves the right and prerogative to deny and/ or restrict the facility and information access of any Contractor employee whose actions are in conflict with the standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom DHS determines to present a risk of compromising sensitive Government information to which he or she would have access under this contract.

The Contractor will report any adverse information coming to their attention concerning contract employees under the contract to the OPR-PSU through the COTR. Reports based on rumor or innuendo should not be made. The subsequent termination of employment of an employee does not obviate the requirement to submit this report. The report shall include the employees' name and social security number, along with the adverse information being reported.

The OPR-PSU must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired DHS issued identification cards and building passes, or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report must be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card. The COTR will return the identification cards and building passes to the responsible ID Unit.

E) Employment Eligibility

The contractor will agree that each employee working on this contract will successfully pass the DHS Employment Eligibility Verification (E-Verify) program operated by USCIS to establish work authorization.

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

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

F) Security Management

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the OPR-PSU through the COTR on all security matters, to include physical, personnel, and protection of all Government information and data accessed by the Contractor.

The COTR and the OPR-PSU shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this contract. Should the COTR determine that the Contractor is not complying with the security requirements of this contract, the Contractor will be informed in writing by the Contracting Officer of the proper action to be taken in order to effect compliance with such requirements.

The following computer security requirements apply to both Department of Homeland Security (DHS) operations and to the former Immigration and Naturalization Service operations (FINS). These entities are hereafter referred to as the Department.

G) Information Technology Security Clearance

When sensitive government information is processed on Department telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in *DHS IT Security Program Publication DHS MD 4300.Pub. or its replacement. Con*tractor personnel must have favorably adjudicated background investigations commensurate with the defined sensitivity level.

Contractors who fail to comply with Department security policy are subject to having their access to Department IT systems and facilities terminated, whether or not the failure results in criminal prosecution. Any person who improperly discloses sensitive information is subject to criminal and civil penalties and sanctions under a variety of laws (e.g., Privacy Act).

H) Information Technology Security Training and Oversight

All contractor employees using Department automated systems or processing Department sensitive data will be required to receive Security Awareness Training. This training will be provided by the appropriate component agency of DHS.

Contractors who are involved with management, use, or operation of any IT systems that handle sensitive information within or under the supervision of the Department, shall receive periodic training at least annually in security awareness and accepted security practices and systems rules of behavior. Department contractors, with significant security responsibilities, shall receive specialized training specific to their security responsibilities annually. The level of training shall be commensurate with the individual's duties and responsibilities and is intended to promote a consistent understanding of the principles and concepts of telecommunications and IT systems security.

All personnel who access Department information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior by personnel accessing systems. Any unauthorized access, sharing of passwords, or other

questionable security procedures should be reported to the local Security Office or Information System Security Officer (ISSO).

16.0DHS HLS EA Compliance

All solutions and services shall meet DHS Enterprise Architecture policies, standards, and procedures as it relates to this Performance Work Statement and associated Task Orders. Specifically, the contractor shall comply with the following Homeland Security Enterprise Architecture (HLS EA) requirements:

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technology Reference Model (TRM) Standards and Products Profile.
- 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.

17.0 Government Points of Contact

Points of contact for this SOW are:

Name	Title	Organization	Telephone Number	Email
Paul Martindale	FPS/SEVP IT Systems Branch Director	ICE/OCIO	202-732-7318	Paul.Martindale@dhs.gov
Carol Wanzer	FPS/SEVP Task Manager	ICE/OCIO	202-732-7320	Carol.R.Wanzer@dhs.gov
Denise Mackie-Smith	ITM Branch Chief	ICE/OI/SEVP	202-305-2090	Denise.Mackie-Smith@dhs.gov
JoNelle M. Hildreth	Contracting Officer	ICE/OAQ	202-307-0077	JoNelle.Hildreth@dhs.gov
TBD	COTR	ICE/OCIO	TBD	TBD

APPENDIX A – List of Acronyms

ADIS	Arrival Departure Information System
AFSP	Alien Flight Student Program
ARO	Alternate Responsible Officer
API	Advance Passenger Information
APIS	Advance Passenger Information System
BTS	Border and Transportation Security
CBP	Customs and Border Protection
CEU	Compliance Enforcement Unit
CIS	Citizenship and Immigration Services
CLAIMS 3	Computer Linked Applications Information Management System
CCD	Consular Consolidated Database
COTS	Commercial off The Shelf
CRU	Case Resolution Unit
DHS	Department of Homeland Security
DOB	Date of Birth
DoJ	Department of Justice
DoS	Department of State
DSO	Designated School Official
ELMS	Electronic Library Management System
FBI	Federal Bureau of Investigation
FTP	File Transfer Protocol
HQ	Headquarters
IBIS	Interagency Border Inspection System
ICE	Immigration and Customs Enforcement
ID	Identifier
IIRIRA	Illegal Immigration Reform and Immigrant Responsibility Act
INA	Immigration and Nationality Act
Intel	Intelligence
ISS	Information System Support
ITARS	I-17 Tracking and Reporting Systems
LPR	Lawful Permanent Resident
MOU	Memorandum of Understanding
NIIS	Nonimmigrant Information System
NIPS	Numerically Integrated Profiling System

NIV	Nonimmigrant Visa
NSEERS	National Security Entry Exit Registration Systems
NTE	Not to Exceed
O&M	Operations and Maintenance
OMB	Office of Management and Budget
PA	Privacy Act
PDSO	Principal Designated School Official
PICS	Password Issuance Control System
Pub. L.	Public Law
POE	Port of Entry
RO	Responsible Officer
SCR	System Change Requests
SBU	Sensitive But Unclassified
SEVIS	Student and Exchange Visitor Information System
SEVP	Student and Exchange Visitor Program
SLM	System Lifecycle Management
SORN	System of Records Notice
SSA	Social Security Administration
SSN	Social Security Number
TSA	Transportation Security Administration
U.S.	United States
USA PATRIOT ACT	Uniting and Strengthening America by Providing Appropriate Tools Required to Interrupt and Obstruct Terrorism Act
US-VISIT	United States Visitor Immigrant Status Indicator Technology

Solicitation/Contract Form

52.203-6 Resriction on Subcontractor Sales to the Government. (SEP 2006) – Alternate I (OCT 1995)

Supplies or Services/Prices

B-1 Items to be Acquired

The Contractor shall furnish all personnel, facilities, equipment, material, supplies, and services (except as may be expressly set forth in this contract as furnished by the Government) and otherwise do all things necessary to, or incident to, performing and providing the following items of work:

Listed in the Statement of Work, Attachment 1

B-2 Contract Pricing

(b)(4)

Description/Specifications

Please refer to the Statement of Work, Attachment 1

Packaging and Marking

Inspection and Acceptance

52.246-5 Inspection of Services - Cost-Reimbursement. (APR 1984)

(a) *Definition.* Services, as used in this clause, includes services performed, workmanship, and material furnished or used in performing services.

(b) The Contractor shall provide and maintain an inspection system acceptable to the Government covering the services under this contract. Complete records of all inspection work performed by the Contractor shall be maintained and made available to the Government during contract performance and for as long afterwards as the contract requires.

(c) The Government has the right to inspect and test all services called for by the contract, to the extent practicable at all places and times during the term of the contract. The Government shall perform inspections and tests in a manner that will not unduly delay the work.

(d) If any of the services performed do not conform with contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, for no additional fee. When the defects in services cannot be corrected by reperformance, the Government may -

(1) Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and

(2) Reduce any fee payable under the contract to reflect the reduced value of the services performed.

(e) If the Contractor fails to promptly perform the services again or take the action necessary to ensure future performance in conformity with contract requirements, the Government may -

(1) By contract or otherwise, perform the services and reduce any fee payable by an amount that is equitable under the circumstances; or

(2) Terminate the contract for default.

(End of clause)

Deliveries or Performance

Please refer to the Statement of Work, Attachment 1 to the Task Order.

Contract Administration Data

G-1 Task Order Administration

The following contact information is provided:

Task Order Contract Specialist (TO CS) (Pre-Award)
Brooke Bernold, (202)616-3246

Task Order Contracting Officer (TO CO) (Pre-Award)
JoNelle Hildreth (202) 307-0077

Task Order Primary Contracting Officer (TO CO) (Post-Award/Administration)
JoNelle Hildreth (202) 307-0077

Task Order Secondary Contracting Officer (TO CO) (Post-Award/Administration)
Brooke Bernold, (202)616-3246

Program Manager (PM)
Paul Martindale, (202) 732-7318

Task Order Contracting Officer Technical Representative
Carol Wanzer (202) 732-7320

Finance Office/Invoice Address
Department of Homeland Security, Immigration and Customs Enforcement
Burlington Finance Center
P.O. Box 1620
Williston, VT 05495-1620
Attn: ICE OCIO-SDD invoice

Task Order Contracting Officer's Technical Representative

The Contracting Officer (CO) will appoint a Task Order Contracting Officer's Technical Representative (COTR) in writing for this task order in accordance with G.2.3 of the EAGLE contract. The COTR will receive, for the Government; all work called for by the task order and will represent the CO in the technical phases of the work. The COTR will provide no supervisory or instructional assistance to contractor personnel.

The COTR is not authorized to change any of the terms and conditions of the contract or the task order. Changes in the scope of work will be made only by the CO by properly executed modifications to the contract or the task order. Additional responsibilities of the COTR include:

Monitoring Performance

The COTR will ensure that the contractor complies with all of the requirements of the statement of work, specifications, or performance work statement, and when requested by the contractor, provide technical direction to the contractor's technical manager. This technical assistance must be within the scope of the contract (e.g., interpreting specifications, statement of work, performance work statement, etc.). When a difference of opinion between you and the contractor occurs, notify the Contracting Officer or the Contract Administrator/Specialist immediately for resolution.

Monitoring Costs

The COTR will review and evaluate the contractor's progress in relation to the expenditures. When the costs expended by the contractor are not commensurate with the contractor's progress, bring this to the attention of the Contracting Officer or contract administrator/specialist for immediate action.

The COTR will review the contractor's invoices/vouchers for reasonableness and applicability to the

contract and recommend to the Contracting Officer approval, conditional approval, or disapproval for payment.

Visits and Meetings With The Contractor

The COTR will make arrangements with the contractor for periodic visits to the contractor's facility to: (1) evaluate the contractor's performance; (2) evaluate changes in the technical performance affecting personnel, the schedule, deliverables, and price or costs; (3) inspect and monitor the use of Government property, if applicable; and (4) ensure that contractor employees being charged to the contract are actually performing the work under the contract. A trip report fully documenting all activities during the visit must be written and a copy provided to the Contracting Officer within three working days after the visit.

Inspection of Contract Items

When notified by the contractor or the Contracting Officer, the COTR will perform, in accordance with the terms of the contract, inspection, acceptance or rejection of the services or deliverables under the contract. Immediately notify the Contracting Officer of all rejections and the reason for the action. The COTR will review progress reports from the Contractor and advise the Contracting Officer of any contractor problems or action required to be taken by the Government.

G-2 Invoicing

(1) Contractors: Please use these procedures when you submit an invoice for all acquisitions from ICE/OAQ. This procedure takes effect 04/01/2008 and pertains to all invoices submitted on that date and thereafter.

1. Invoices shall now be submitted via one of the following three methods:

a. By mail: DHS, ICE
Burlington Finance Center
P.O. Box 1620
Williston, VT 05495-1620
Attn: ICE OCIO-SDD invoice

b. By facsimile (fax) at: 802-288-7658 (include a cover sheet with point of contact & # of pages)

c. By e-mail at: Invoice.Consolidation@dhs.gov

Invoices submitted by other than these three methods will be returned. Contractor Taxpayer Identification Number (TIN) must be registered in the Central Contractor Registration (http://www.ccr.gov) prior to award and shall be notated on every invoice submitted to ICE/OAQ on or after 04/01/2008 to ensure prompt payment provisions are met. The ICE program office identified in the delivery order/contract shall also be notated on every invoice. Please send an additional copy of the invoice to ICEOCIOITSRACQ@DHS.GOV.

2. In accordance with FAR 52.232-25 (a)(3), Prompt Payment, the information required with each invoice submission is as follows:

An invoice must include:
(i) Name and address of the Contractor;
(ii) Invoice date and number;
(iii) Contract number, contract line item number and, if applicable, the order number;
(iv) Description, quantity, unit of measure, unit price and extended price of the items delivered;
(v) Shipping number and date of shipment, including the bill of lading number and weight of shipment if

shipped on Government bill of lading;
(vi) Terms of any discount for prompt payment offered;
(vii) Name and address of official to whom payment is to be sent;
(viii) Name, title, and phone number of person to notify in event of defective invoice; and
(ix) Taxpayer Identification Number (TIN). The Contractor shall include its TIN on the invoice only if required elsewhere in this contract. (See paragraph 1 above.)
(x) Electronic funds transfer (EFT) banking information.
(A) The Contractor shall include EFT banking information on the invoice only if required elsewhere in this contract.
(B) If EFT banking information is not required to be on the invoice, in order for the invoice to be a proper invoice, the Contractor shall have submitted correct EFT banking information in accordance with the applicable solicitation provision, contract clause (e.g., 52.232-33, Payment by Electronic Funds Transfer; Central Contractor Registration, or 52.232-34, Payment by Electronic Funds Transfer; Other Than Central Contractor Registration), or applicable agency procedures.
(C) EFT banking information is not required if the Government waived the requirement to pay by EFT.

Invoices without the above information may be returned for resubmission.

Receiving Officer/COTR: Each Program Office is responsible for acceptance and receipt of goods and/or services. Upon receipt of goods/services, complete the applicable FFMS reports or DFC will not process the payment.

Special Contract Requirements

Contract Clauses

52.204-9 Personal Identity Verification of Contractor Personnel. (SEP 2007)

52.217-8 Option to Extend Services . (NOV 1999)

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

(End of clause)

52.217-9 Option to Extend the Term of the Contract. (MAR 2000)

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

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

(c) The total duration of this contract, including the exercise of any options under this clause, shall not exceed 60 months (5 years).

(End of clause)

52.232-19 Availability of Funds for the Next Fiscal Year. (APR 1984)

Funds are not presently available for performance under this contract beyond 09/30/2009. The Government's obligation for performance of this contract beyond that date is contingent upon the availability of appropriated funds from which payment for contract purposes can be made. No legal liability on the part of the Government for any payment may arise for performance under this contract beyond 09/30/2009, until funds are made available to the Contracting Officer for performance and until the Contractor receives notice of availability, to be confirmed in writing by the Contracting Officer.

(End of Clause)

52.219-8 Utilization of Small Business Concerns. (MAY 2004)

52.219-9 Small Business Subcontracting Plan. (NOV 2007)

52.225-13 Restrictions on Certain Foreign Purchases. (FEB 2006)

52.227-14 Rights in Data--General. (DEC 2007)

52.232-22 Limitation of Funds (APR 1984)

52.233-4 Applicable Law for Breach of Contract Claim. (OCT 2004)

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

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

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

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

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

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

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

(e) Within 6 months after contract award, the contractor shall submit written proof of IT Security accreditation to DHS for approval by the DHS Contracting Officer. Accreditation will proceed according to the criteria of the DHS Sensitive System Policy Publication, 4300A (Version 2.1, July 26, 2004) or any replacement publication, which the Contracting Officer will provide upon request. This accreditation will include a final security plan, risk assessment, security test and evaluation, and disaster recovery plan/continuity of operations plan. This accreditation, when accepted by the Contracting Officer, shall be incorporated into the contract as a compliance document. The contractor shall comply with the approved accreditation documentation.

(End of clause)

3052.204-71 Contractor employee access. (JUN 2006) -- Alternate I (JUN 2006)

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

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

(2) Sensitive Security Information (SSI), as defined in Title 49, Code of Federal Regulations, part 1520, as amended, Policies and Procedures of Safeguarding and Control of SSI, as amended, and any supplementary guidance officially communicated by an authorized official of the Department of Homeland Security (including the Assistant Secretary for the Transportation Security Administration or his/her designee);

(3) Information designated as For Official Use Only, which is unclassified information of a sensitive nature and the unauthorized disclosure of which could adversely impact a person's privacy or welfare, the conduct of Federal programs, or other programs or operations essential to the national or homeland security interest; and

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

(b) Information Technology Resources include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

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

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

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

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

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

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

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

> (1) The individual must be a legal permanent resident of the U.S. or a citizen of Ireland, Israel, the Republic of the Philippines, or any nation on the Allied Nations List maintained by the Department of State;
>
> (2) There must be a compelling reason for using this individual as opposed to a U.S.

citizen; and

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

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

(End of clause)

3052.209-70 Prohibition on contracts with corporate expatriates. (JUN 2006)

(a) Prohibitions.

Section 835 of the Homeland Security Act, 6 U.S.C. 395, prohibits the Department of Homeland Security from entering into any contract with a foreign incorporated entity which is treated as an inverted domestic corporation as defined in this clause, or with any subsidiary of such an entity. The Secretary shall waive the prohibition with respect to any specific contract if the Secretary determines that the waiver is required in the interest of national security.

(b) Definitions. As used in this clause:

Expanded Affiliated Group means an affiliated group as defined in section 1504(a) of the Internal Revenue Code of 1986 (without regard to section 1504(b) of such Code), except that section 1504 of such Code shall be applied by substituting `more than 50 percent' for `at least 80 percent' each place it appears.

Foreign Incorporated Entity means any entity which is, or but for subsection (b) of section 835 of the Homeland Security Act, 6 U.S.C. 395, would be, treated as a foreign corporation for purposes of the Internal Revenue Code of 1986.

Inverted Domestic Corporation. A foreign incorporated entity shall be treated as an inverted domestic corporation if, pursuant to a plan (or a series of related transactions)

(1) The entity completes the direct or indirect acquisition of substantially all of the properties held directly or indirectly by a domestic corporation or substantially all of the properties constituting a trade or business of a domestic partnership;

(2) After the acquisition at least 80 percent of the stock (by vote or value) of the entity is held

(i) In the case of an acquisition with respect to a domestic corporation, by former shareholders of the domestic corporation by reason of holding stock in the domestic corporation; or

(ii) In the case of an acquisition with respect to a domestic partnership, by former partners of the domestic partnership by reason of holding a capital or profits interest in the domestic partnership; and

(3) The expanded affiliated group which after the acquisition includes the entity does not have substantial business activities in the foreign country in which or under the law of which the entity is created or organized when compared to the total business activities of such expanded affiliated group.

Person, domestic, and foreign have the meanings given such terms by paragraphs (1), (4), and (5) of section 7701(a) of the Internal Revenue Code of 1986, respectively.

(c) Special rules. The following definitions and special rules shall apply when determining whether a foreign incorporated entity should be treated as an inverted domestic corporation.

(1) *Certain Stock Disregarded.* For the purpose of treating a foreign incorporated entity as an inverted domestic corporation these shall not be taken into account in determining ownership:

(i) Stock held by members of the expanded affiliated group which includes the foreign incorporated entity; or

(ii) stock of such entity which is sold in a public offering related to the acquisition described in subsection (b)(1) of Section 835 of the Homeland Security Act, 6 U.S.C. 395(b)(1).

(2) *Plan Deemed In Certain Cases*. If a foreign incorporated entity acquires directly or indirectly substantially all of the properties of a domestic corporation or partnership during the 4-year period beginning on the date which is 2 years before the ownership requirements of subsection (b)(2) are met, such actions shall be treated as pursuant to a plan.

(3) *Certain Transfers Disregarded.* The transfer of properties or liabilities (including by contribution or distribution) shall be disregarded if such transfers are part of a plan a principal purpose of which is to avoid the purposes of this section.

(d) *Special Rule for Related Partnerships*. For purposes of applying section 835(b) of the Homeland Security Act, 6 U.S.C. 395(b) to the acquisition of a domestic partnership, except as provided in regulations, all domestic partnerships which are under common control (within the meaning of section 482 of the Internal Revenue Code of 1986) shall be treated as a partnership.

(e) Treatment of Certain Rights.

(1) Certain rights shall be treated as stocks to the extent necessary to reflect the present value of all equitable interests incident to the transaction, as follows:

(i) warrants;

(ii) options;

(iii) contracts to acquire stock;

(iv) convertible debt instruments; and

(v) others similar interests.

(2) Rights labeled as stocks shall not be treated as stocks whenever it is deemed appropriate to do so to reflect the present value of the transaction or to disregard transactions whose recognition would defeat the purpose of Section 835.

(f) *Disclosure.* The offeror under this solicitation represents that (Check one):

__ it is not a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73;

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it has submitted

a request for waiver pursuant to 3009.104-74, which has not been denied; or

__ it is a foreign incorporated entity that should be treated as an inverted domestic corporation pursuant to the criteria of (HSAR) 48 CFR 3009.104-70 through 3009.104-73, but it plans to submit a request for waiver pursuant to 3009.104-74.

(g) A copy of the approved waiver, if a waiver has already been granted, or the waiver request, if a waiver has been applied for, shall be attached to the bid or proposal.

(End of provision)

3052.211-70 Index for specifications. (DEC 2003)

If an index or table of contents is furnished in connection with specifications, it is understood that such index or table of contents is for convenience only. Its accuracy and completeness is not guaranteed, and it is not to be considered as part of the specifications. In case of discrepancy between the index or table of contents and the specifications, the specifications shall govern.

(End of clause)

3052.215-70 Key personnel or facilities. (DEC 2003)

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

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

The Key Personnel or Facilities under this Contract:

Configuration Management Lead
Data Architect
Security Engineer
Solution Development Lead
Program Manager
Systems Engineer Lead

3052.219-70 Small business subcontracting plan reporting. (JUN 2006)

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

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

(End of clause)

3052.242-72 Contracting officer's technical representative. (DEC 2003)

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

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

(End of clause)

3052.245-70 Government property reports. (JUN 2006)

(a) The Contractor shall prepare an annual report of Government property in its possession and the possession of its subcontractors.

(b) The report shall be submitted to the Contracting Officer not later than September 15 of each calendar year on DHS Form 0700-5, Contractor Report of Government Property.

(End of clause)

3052.237-71 Information Technology Systems Access for Contractors

INFORMATION TECHNOLOGY SYSTEMS ACCESS FOR CONTRACTORS
(NOV 2004) (Deviation)

(a) "Sensitive Information" means information that is:

(1) Protected Critical Infrastructure Information (PCII) as described in the Critical Infrastructure Information Act of 2002, 6 U.S.C. sections 211-224; its implementing regulations, 6 CFR Part 29; or the applicable PCII Procedures Manual; or

(2) Sensitive Security Information (SSI), as described in 49 CFR Part 1520; or

(3) Sensitive but Unclassified Information (SBU), which consists of any other unclassified information which:

(i) if lost, misused, modified, or accessed without authorization, could adversely affect the national interest, proprietary rights, the conduct of Federal programs, or individual privacy under 5 U.S.C. section 552a; and,

(ii) if provided by the government to the contractor, is marked in such a way as to place a reasonable person on notice of its sensitive nature.

(b) ¿Information Technology Resources¿ include, but are not limited to, computer equipment, networking equipment, telecommunications equipment, cabling, network drives, computer drives, network software, computer software, software programs, intranet sites, and internet sites.

(c) Contractor employees working on this contract must complete such forms, as may be necessary for security or other reasons, including the conduct of background investigations to determine suitability. Completed forms shall be submitted as directed by the Contracting Officer. Upon the Contracting Officer's request, the Contractor's employees shall be fingerprinted, or subject to other investigations as required. All contractor employees requiring recurring access to Government facilities or access to sensitive information or IT resources are required to have a favorably adjudicated background investigation prior to commencing

work on this contract unless this requirement is waived under Departmental procedures.

(d) The Contracting Officer may require the contractor to prohibit individuals from working on the contract if the government deems their initial or continued employment contrary to the public interest for any reason, including, but not limited to, carelessness, insubordination, incompetence, or security concerns.

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

(f) 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 personnel who are non-U.S. citizen after contract award shall also be reported to the contracting officer.

(g) 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.

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

(i) The contractor shall have access only to those areas of DHS Organizational Element (OE) 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.

(j) Contractor access to DHS networks from a remote location is a temporary privilege for mutual convenience while the contractor performs business for the DHS OE. It is not a right, a guarantee of access, a condition of the contract, nor is it Government Furnished
Equipment (GFE).

(k) 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.

(l) Non-U.S. citizens shall not be authorized to access or assist in the development, operation, management or maintenance of Department IT systems under the contract, unless a waiver has been granted by the Head of the Organizational Element or designee, with the concurrence of the Office of Security and Departments CIO or designee. In order for a waiver to be granted:
(i) 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.
(ii) All required security forms specified by the government and any necessary background check must be satisfactorily completed.
(iii) There must be a compelling reason for using this individual as opposed to a U.S. citizen.
(iv) The waiver must be in the best interest of the Government.

List of Documents, Exhibits and Other Attachments

Attachment 1 – Statement of Work