Company Name:
O’Neal Technologies

Contract Number:
GS-35F-0113T (GS35F0113T)

Order Number:
HSCETC-08-F-00027 (HSCETC08F00027)

Requisition Number:
SDD-08-AF07 (SDD08AF07)

Period of Performance:
9/25/2008 through 9/24/2011

Services Provided:
Independent Verification & Validation (IV&V); Services in Support of the Risk Assessment and Management Program (RAMP) for the Federal Protective Service (FPS).

SOLICITATION/CONTRACT/ORDER FOR COMMERCIAL ITEMS

OFFEROR TO COMPLETE BLOCKS 12, 17, 23, 24, & 30

1. REQUISITION NUMBER	PAGE	OF
SDD-08-AF07	1	5

2. CONTRACT NO.	3. AWARD/ EFFECTIVE DATE	4. ORDER NUMBER	5. SOLICITATION NUMBER	6. SOLICITATION ISSUE DATE
GS-35F-0113T		HSCETC-08-F-00027		

7. FOR SOLICITATION INFORMATION CALL:	a. NAME	b. TELEPHONE NUMBER (No collect calls)	8. OFFER DUE DATE/LOCAL TIME
	Ben Branch	b2Low	

9. ISSUED BY CODE ICE/TC/IT SE

ICE/Info Tech Svs/IT Services
Immigration and Customs Enforcement
Office of Acquisition Management
425 I Street NW, Suite 2208
Washington DC 20536

10. THIS ACQUISITION IS

☐ UNRESTRICTED OR ☒ SET ASIDE: 100.00 % FOR:

☐ SMALL BUSINESS ☐ EMERGING SMALL BUSINESS

NAICS:

☒ HUBZONE SMALL BUSINESS

SIZE STANDARD:

☐ SERVICE-DISABLED VETERAN-OWNED SMALL BUSINESS ☐ 8(A)

11. DELIVERY FOR FOB DESTINATION UNLESS BLOCK IS MARKED

☐ SEE SCHEDULE

12. DISCOUNT TERMS

b2Low

☐ **13a.** THIS CONTRACT IS A RATED ORDER UNDER DPAS (15 CFR 700)

13b. RATING

14. METHOD OF SOLICITATION

☐ RFQ ☐ IFB ☐ RFP

15. DELIVER TO CODE ICE/CIO

ICE Chief Information Officer
Immigration and Customs Enforcement
801 I Street, NW
Suite 700
Washington DC 20536

16. ADMINISTERED BY CODE ICE/TC/IT SERV

ICE/Info Tech Svs/IT Services
Immigration and Customs Enforcement
Office of Acquisition Management
425 I Street NW, Suite 2208
Attn: Ben Branch
Washington DC 20536

17a. CONTRACTOR/ OFFEROR CODE 0267929080000 FACILITY CODE

ONEAL TECHNOLOGIES INC
13090 SALFORD TERRACE
UPPER MARLBORO MD 207726133

TELEPHONE NO.

18a. PAYMENT WILL BE MADE BY CODE ICE-OCIO-SDD

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

☐ **17b.** CHECK IF REMITTANCE IS DIFFERENT AND PUT SUCH ADDRESS IN OFFER

18b. SUBMIT INVOICES TO ADDRESS SHOWN IN BLOCK 18a UNLESS BLOCK BELOW IS CHECKED ☐ SEE ADDENDUM

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	DUNS Number: 026792908 COTR: Eric Simpson b2Low b6 Contract Specialist: Ben Branch b2Low b6 *(Use Reverse and/or Attach Additional Sheets as Necessary)*				

25. ACCOUNTING AND APPROPRIATION DATA

See schedule

26. TOTAL AWARD AMOUNT *(For Govt. Use Only)*

$632,444.80

☐ 27a. SOLICITATION INCORPORATES BY REFERENCE FAR 52.212-1, 52.212-4. FAR 52.212-3 AND 52.212-5 ARE ATTACHED. ADDENDA ☐ ARE ☐ ARE NOT ATTACHED

☒ 27b. CONTRACT/PURCHASE ORDER INCORPORATES BY REFERENCE FAR 52.212-4. FAR 52.212-5 IS ATTACHED. ADDENDA ☐ ARE ☒ ARE NOT ATTACHED

☐ 28. CONTRACTOR IS REQUIRED TO SIGN THIS DOCUMENT AND RETURN _____ COPIES TO ISSUING OFFICE. CONTRACTOR AGREES TO FURNISH AND DELIVER ALL ITEMS SET FORTH OR OTHERWISE IDENTIFIED ABOVE AND ON ANY ADDITIONAL SHEETS SUBJECT TO THE TERMS AND CONDITIONS SPECIFIED HEREIN.

☒ 29. AWARD OF CONTRACT REF. _____ OFFER DATED _____. YOUR OFFER ON SOLICITATION (BLOCK 5), INCLUDING ANY ADDITIONS OR CHANGES WHICH ARE SET FORTH HEREIN, IS ACCEPTED AS TO ITEMS:

30a. SIGNATURE OF OFFEROR/CONTRACTOR	31a. UNITED STATES OF AMERICA *(SIGNATURE OF CONTRACTING OFFICER)*

30b. NAME AND TITLE OF SIGNER *(Type or print)*	30c. DATE SIGNED	31b. NAME OF CONTRACTING OFFICER *(Type or print)*	31c. DATE SIGNED
		Paul T. Osterhaus	9/25/08

AUTHORIZED FOR LOCAL REPRODUCTION
PREVIOUS EDITION IS NOT USABLE

STANDARD FORM 1449 (REV. 3/2005)
Prescribed by GSA - FAR (48 CFR) 53.212

19. ITEM NO.	20. SCHEDULE OF SUPPLIES/SERVICES	21. QUANTITY	22. UNIT	23. UNIT PRICE	24. AMOUNT
	Contracting Officer: Paul Osterhaus b2Low b6 This is a Firm Fixed Price Task Order issued against GSA Federal Supply Schedule GS-35F-0113T. All Terms and Conditions of GS-35F-0113T apply. , please use these procedures when you submit an invoice for all acquisitions emanating from ICE/OAQ. 1. In accordance with Section G, Contract Administration Data, 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 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 Continued ...				

32a. QUANTITY IN COLUMN 21 HAS BEEN

☐ RECEIVED ☐ INSPECTED ☐ ACCEPTED, AND CONFORMS TO THE CONTRACT, EXCEPT AS NOTED: _____

32b. SIGNATURE OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32c. DATE	32d. PRINTED NAME AND TITLE OF AUTHORIZED GOVERNMENT REPRESENTATIVE

32e. MAILING ADDRESS OF AUTHORIZED GOVERNMENT REPRESENTATIVE	32f. TELEPHONE NUMBER OF AUTHORIZED GOVERNMENT REPRESENTATIVE
	32g. E-MAIL OF AUTHORIZED GOVERNMENT REPRESENTATIVE

33. SHIP NUMBER	34. VOUCHER NUMBER	35. AMOUNT VERIFIED CORRECT FOR	36. PAYMENT	37. CHECK NUMBER
☐ PARTIAL ☐ FINAL			☐ COMPLETE ☐ PARTIAL ☐ FINAL	

38. S/R ACCOUNT NUMBER	39. S/R VOUCHER NUMBER	40. PAID BY

41a. I CERTIFY THIS ACCOUNT IS CORRECT AND PROPER FOR PAYMENT		42a. RECEIVED BY *(Print)*	
41b. SIGNATURE AND TITLE OF CERTIFYING OFFICER	41c. DATE	42b. RECEIVED AT *(Location)*	
		42c. DATE REC'D *(YY/MM/DD)*	42d. TOTAL CONTAINERS

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	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. The ICE program office identified in the delivery order/contract shall also be notated on every invoice. 2. In accordance with Section I, Contract Clauses, FAR 52.212-4 (g)(1), Contract Terms and Conditions, Commercial Items, or FAR 52.232-25 (a)(3), Prompt Payment, as applicable, 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 Continued ...				

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	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. 3. All other terms and conditions remain the same. 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. The following Federal Acquisition Regulation clauses are hereby incorporated by reference: FAR 52.217-8 Option to Extend Services FAR 52.217-9 Option to Extend the Term of the Contract The Statement of Work dated September 18, 2008 is hereby incorporated by attachment. Accounting Info: b2Low Period of Performance: 09/25/2008 to 09/24/2011				
0001	RAMP IV&V Base Year Fixed Price	1	EA	632,444.80	632,444.80
0002	RAMP IV&V Option Year One Fixed Price Amount: $664,568.00(Option Line Item) 09/24/2009				0.00
0003	RAMP IV&V Option Year Two Fixed Price Amount: $698,246.40(Option Line Item) 09/24/2010				0.00
	Continued ...				

NAME OF OFFEROR OR CONTRACTOR

ONEAL TECHNOLOGIES INC

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)
	The total amount of award: $1,995,259.20. The obligation for this award is shown in box 26.				

U.S. Department of Homeland Security [DHS]
Immigration and Customs Enforcement [ICE]
Federal Protective Service [FPS]
&
Office of the Chief Information Officer [OCIO]

Statement of Work

Independent Verification & Validation (IV&V) Services In Support of the Risk Assessment and Management Program (RAMP) for

Federal Protective Service (FPS)

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

Table of Contents

1.0 PROJECT TITLE

Independent Verification & Validation Services in Support of the Risk Assessment and Management Program (RAMP).

2.0 BACKGROUND

FPS is responsible for mitigating risk to Federal facilities and their occupants. FPS achieves this mission for more than 8,800 Federal facilities nationwide by conducting regular risk assessments, recommending and implementing countermeasures to reduce risk, and providing critical response and training services for Federal stakeholders.

FPS' work focuses directly on the interior security of the nation; reducing the risks posed to federal facilities throughout the nation. Uniformed FPS Inspectors conduct risk assessments, respond to calls for assistance, perform investigations, provide crime prevention tips, and assist in occupant emergency planning.

All federal facilities owned or leased by the General Services Administration (GSA) receive a thorough Building Security Assessment (BSA) on a recurring schedule. During this assessment, representatives of agencies in the facility are interviewed to gather information on the specific mission they perform within the facility and intelligence and crime statistics for the area are reviewed, as are existing security countermeasures. Based on the findings, and working with the agencies housed in the facility, security countermeasures are added or adjusted. This allows tailored security for each individual facility versus a one-size-fits-all approach.

The Risk Assessment and Management Program (RAMP) system will be the primary tool used by FPS Inspectors to fulfill their mission of securing federal facilities and ensuring occupants are safe. RAMP is envisioned as a comprehensive, systematic, and dynamic means of capturing, accessing, storing, managing, and utilizing pertinent facility threat, vulnerability, consequence, and countermeasure information.

The operational vision of RAMP is that an Inspector will have a portable device that will serve as the platform to access RAMP. The Inspector will be able to carry the device during a BSA, perhaps mount it in his vehicle, and carry it to his office. RAMP will be entirely web-enabled and accessible anywhere in the U.S. via a secure wireless connection. The system will guide the Inspector through the assessment process, collecting standardized data on all Federal facilities. The data collected will be used to automatically generate reports and required documentation. RAMP will provide information that will enable the Inspector to make informed, objective, and defensible decisions when recommending countermeasures to reduce the impact of credible threats to their facilities. Selected countermeasures will be tracked in RAMP throughout their lifecycle. FPS management will use analytical tools in RAMP to access real time, accurate data to ensure they can make timely, key decisions.

RAMP will be developed to replace 3 IT systems that are in place today at FPS. A short description of each system is listed below:

- Federal Security Risk Manager (FSRM) – FSRM is the CD-based application that is used to create BSA reports. It allows Inspectors to enter information collected during an assessment and generates a BSA report based on standard phrasing with a standard layout. There is no central data repository for this information; it resides on each Inspector's laptop until it is copied to a regional shared drive. FSRM does not provide quantitative measurements for risk either; risk indicators are determined by the Inspector.
- Security Tracking System (STS) – STS is the system that maintains information on all countermeasures that are installed at facilities that FPS assesses.
- Contract Guard Employment Requirements Tracking System (CERTS) – CERTS is the system that maintains information on contract guard certifications. These certifications help FPS to determine whether contract guards are qualified to work for FPS.

At its core, RAMP must meet the following objectives:

- Compatible with a new, rigorous, quantitative risk assessment methodology that supports the National Infrastructure Protection Plan (NIPP) and Interagency Security Committee (ISC) standards. This methodology is expected to become the standard for use by multiple stakeholders and be applicable for the majority of government buildings at the federal, state, and local levels.
- Implement standardized FPS business processes and systems supporting the BSA program to better meet the needs of the agency and its clients by enhancing productivity and significantly improving customer service.
- Incorporate this methodology and business processes in a web-enabled application with an appropriate central data repository for use not only by FPS but also potentially by those performing such functions for other government agencies.
- Utilize the current DHS enterprise architecture (EA) structure, creating 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 information).

Improving the efficiency and effectiveness of services to its customers, RAMP will provide FPS the ability to fulfill its Vision – Secure Facilities and Safe Occupants – by mitigating risk to Federal facilities and their occupants. RAMP

will be the central repository of record providing accurate and efficient access of real time information to FPS resources and key users/stakeholders.

3.0 SCOPE OF WORK

The specific objective of the proposed task order is to provide an Independent Verification and Validation (IV&V) for all software developed and hardware prepared for RAMP as part of the "Software Development Services in Support of the Risk Assessment and Management Program (RAMP)" effort. This statement of work details the requirements to provide the required IV&V support.

4.0 APPLICABLE DOCUMENTS

4.1 Technical Documents

The technical documents below are applicable to this SOW and will 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 Standards Profile
- RAMP Functional Requirements Document

4.2 Other Supporting Documentation and Guidance

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

- 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.
- Federal Protective Service Risk Assessment and Management Methodology, 2008
- National Infrastructure Protection Plan, 2006
- National Infrastructure Protection Plan Sector-Specific Plan - Government Facilities Sector

- ISC Security Standards for Leased Space
- ISC Security Design Criteria for New Federal Office Buildings and Major Modernization Projects
- ISC Minimum Standards for Federal Building Access Procedures
- ISC Safe Practices for Safe Mail Handling
- Vulnerability Assessment of Federal Facilities

5.0 SPECIFIC TASKS

This section outlines the specific tasks that the Contractor is required to execute. Tasks are organized according to high-level categories.

The primary task required of the Contractor is to verify and validate that all formal "Software Development Services in Support of the Risk Assessment and Management Program (RAMP)" requirements are satisfied. The remainder of this section provides further detail.

5.1 Standards and Processes

Independent verification and validation of the software applications developed and maintained by RAMP is an important part of the software development process for RAMP. IV&V is the process of verifying that the output of each piece of software meets the requirements that were established for it prior to its development, and validating that the software, at the end of the development effort, meets the overall project objectives. IV&V must be performed in an environment independent of any influence or control from the development effort. This will help assure that the software is being developed properly and accurately.

IV&V for this effort will consist of at least the following tasks:

- The Contractor shall verify that prescribed ICE processes and procedures – most notably, ICE System Lifecycle Management (SLM) – are used to develop RAMP software. Exceptions or deviations from ICE guidance must be approved by the Government.
- The Contractor shall verify that all documents and deliverables required by ICE – most notably, from the ICE SLM Handbook – are produced and approved according to project schedule. Exceptions or deviations from ICE guidance must be approved by the Government.
- The Contractor shall verify and validate all plans and deliverables associated with the "Software Development Services in Support of the Risk Assessment and Management Program (RAMP)" effort.
- The Contractor shall use their expertise with CMMI Level 3 (or higher) processes to evaluate the processes used to develop the RAMP

software and hardware solution. The Contractor shall be capable of evaluating CMMI Level 2, 3, and 4 compliance.

5.2 Configuration Management

The Contractor shall:

- Verify that all documentation is under configuration control in the configuration control system recommended by ICE OCIO Architecture Division and formally approved upon delivery to Government.
- Verify that all design products are under configuration control in the configuration control system recommended by ICE OCIO Architecture Division and formally approved before coding begins.
- Verify that developed code is under configuration control in the configuration control system recommended by ICE OCIO Architecture Division and is easily accessible by developers.

5.3 Software Development

The Contractor shall:

Design

- Verify that high-level design products are workable and efficient, and that they satisfy all system requirements.
- Verify that the design and analysis process used to develop the design complies with ICE processes (i.e. SLM).
- Verify that design products can be traced back to system requirements.
- Verify that all required documents are produced accurately and according to schedule.

Code

- Verify that ICE standards and processes (especially SLM) are followed during coding.
- Verify that developed code is maintainable, taking into account software metrics including but not limited to modularity, complexity, and source and object size.
- Evaluate code documentation for quality, completeness (including maintenance history), and accessibility.
- Verify that code complies with ICE coding standards and guidelines. This includes, but is not limited to, structure, documentation, modularity, naming conventions, and format of the code.
- Verify that all software requirements are satisfied.

Testing

- Verify that the plans, requirements, environment, tools, and procedures used for testing system modules are complete and satisfy all testing requirements.
- Verify that testing plans are executed properly.
- Verify that an appropriate level of test coverage is achieved by the test process, that test results are verified, that the correct code configuration has been tested, and that the tests are appropriately documented.

5.4 Data Migration and Transition

The Contractor shall perform the following:

- Verify that the Data Migration Plan and Transition Plan properly communicate feasible, efficient, and satisfactory migration and transition activities.
- Verify that data migration is performed according to Government-approved Data Migration guidance
- Verify that transition is performed according to Government-approved Data Migration

5.5 Hardware Integration

The Contractor shall perform the following:

- Verify that various proposals are provided for a solution with software and hardware (portable devise) components. Verify that proposed portable devices satisfy all requirements for portable device.
- Verify that the required number of portable devices are procured
- Verify that portable devices are configured properly so that they are usable to Inspectors.
- Verify that portable devices are deployed according to Government-approved Deployment Plan
- Verify that the portable device can be used to access the RAMP application. This involves simulating real-world situations such as carrying the laptop and using the RAMP application while walking around a building.

5.6 Operations and Maintenance (O&M)

Activities for Operations and Maintenance will commence after Year 1 of the development of the system. At this stage the system will be in production.

The Contractor shall perform the following tasks:

- Verify that performance and implementation failures are corrected
- Verify that emergency repairs are performed when immediate correction is necessary
- Verify that enhancements are performed according to Government direction
- Verify that Tier 1 Help Desk requirements are satisfied, including providing the ICE Help Desk with updated information and help desk protocols
- Verify that Tier 2 and 3 Help Desk requirements are satisfied, including providing help desk services over the telephone

5.7 System Change Requests

The Contractor shall:

- Verify that the approved System Change Request (SCR) process is followed.
- Verify that the ICE approved tracking system (current requirement is Serena Tracker) is used for all SCRs.
- Verify that required documentation for all System Change Requests (SCRs) is produced

5.8 Training

The Contractor shall:

- Verify that an acceptable training plan is developed and executed.
- Verify that training materials are user-friendly
- Verify that all training is conducted on-time
- Verify that training materials and training sessions are developed in conjunction with FPS and representatives from Federal Law Enforcement Training Center (FLETC) Physical Security Academy (PSA).

6.0 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 below:

6.1 Deliverables Summary and Metrics

Deliverable	Frequency	Copies	Recipients
IV&V Management Plan	To be completed within 30 days from the date the Contractor is notified of contract approval As Required	2 CDs 1 PC	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
Initial Review Report	Review to commence within 60 days from the date the Contractor is notified of contract approval. Report to be delivered 60 days after the review commences.	2 CDs 1PC	TM (2) copy/ COTR (1) copy / CO (trans ltr.)
Periodic Review Report(s)	As Required	2 CDs 1 PC	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
Formal presentation(s) on the IV&V project components to Stakeholders	As Required	2 CDs 1 PC	TM (3) copy/ COTR (trans ltr.), CO (trans ltr.)
Weekly Progress Reports	Weekly	1 electronic copy	TM (1) copy/ COTR (1) copy/ CO (trans ltr.)
Monthly Progress Reports	Monthly	1 electronic copy	TM (1) copy/ COTR (1) copy/ CO (trans ltr.)

6.2 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 selected contractor for IV&V work should work closely with the selected contractor for RAMP Software Development to help propose, procure, integrate, and deploy all hardware requirements dictated by the

6.3 Progress Reports, Status Reports & Program Reviews

6.3.1 Weekly Progress Reports

The Contractor shall prepare a weekly progress report. Initial reports are due to the COTR 14 days after award and every 7 days thereafter until the last week of performance. The weekly report shall include but not be limited to the following:

- Description of work planned
- Description of work accomplished
- Analysis of the difference between planned and accomplished
- Work planned for the following week
- Outstanding issues

6.3.2 Monthly 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 include but not be limited to the following:

- Status of risks identified
- Funding, earned value reporting, and burn rate
- Status of the high level milestones
- Personnel, logistical, and contracting issues
- Other open issues

6.3.3 Quarterly Status Report

The Contractor shall prepare quarterly status report for the ICE/OCIO Project Manager and the COTR. Generally, these reports shall include accomplishments, any deviations from planned activities, field related issues, other issues, and planned activities for the next period. The reports are for the PM 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.

6.3.4 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 shall require only minimal presentation time.

6.3.5 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.

6.4 Financial Reporting

The Contractor shall submit monthly reports to the ICE COTR that must be prepared in sufficient detail to support OMB A-11 reporting requirements at Exhibits 53 and 300. The report is due on the 10th business day of each calendar month, starting with the second calendar month after Contract award. The initial report shall cover the first calendar month of Contract performance. Subsequent reports will be provided monthly and shall cover the calendar month 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:

1. Cost Ceiling, Proposal Burn rate, Proposal Cumulative, Funding Ceiling
2. Monthly Incurred, Cumulative Incurred
3. Monthly Outlook, Total Estimated Cost
4. 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.

6.5 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.

6.6 Quality Assurance Reports

The Contractor will be required to develop the format for the Quality Assurance Report and obtain approval from the Government prior to delivery of the first Quality Assurance Report. 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.

6.7 Ad Hoc Deliverables

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

6.8 Product Acceptance

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 if they are not accepted or rejected within the ten working day period.

7.0 GOVERNMENT FURNISHED EQUIPMENT AND INFORMATION

A zip file with all available documentation relevant to RAMP will be provided to the Contractor upon release of the SOW. Upon award (and obtaining required security clearance), the Contractor shall 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.

8.0 PLACE OF PERFORMANCE

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 EST, Monday through Friday except federal holidays, unless otherwise authorized by the ICE Task Manager.

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.

9.0 PERIOD OF PERFORMANCE

The RAMP IV&V effort will consist of a twelve-month base period and two twelve-month option periods. The base period will begin upon award. The following table identifies activities that the Contractor will perform during each contract period.

Period	Duration	Activities
Base year	12 months	• IV&V Services
Option year 1	12 months	• IV&V Services
Option year 2	12 months	• IV&V Services

10.0 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.

11.0 KEY PERSONNEL REQUIREMENTS

The Contractor shall provide resumes along with the proposal for all full-time key personnel, where key personnel are defined as the Project Manager and Lead IV&V Analyst. The resumes shall include the experience and skills of the key personnel proposed for the tasks. The key personnel who actually will work on the project shall be specified by name. The Contractor and the COTR must agree

that the key personnel are critical to the performance of the contract and cannot be removed without COTR approval. The COTR has the right of refusal for any personnel assigned to these tasks.

Key personnel shall only be replaced with people of comparable skill and experience level, and the Contractor shall obtain approval from the Government prior to any key personnel replacement.

Upon contract award, resumes must be provided for all personnel who will be working on the project. Approval from the Government for all personnel shall be obtained before work may begin.

12.0 GOVERNMENT POINTS OF CONTACT

Points of contact for this SOW are:

Name	Title	Organization	Telephone Number	Email
JoNelle M. Hildreth	Contracting Officer	ICE/OAQ	202-307-0077	JoNelle.M.Hildreth@dhs.gov
Ben Branch	Contract Ben Branch	ICE/OAQ	202-353-2503	Ben.Branch@dhs.gov
TBD	COTR	ICE/OCIO		
TBD	Program Manager	ICE/OCIO		
TBD	Project Manager	ICE/OCIO		
TBD	Business Owner	ICE/FPS		

13.0 ACCESSIBILITY REQUIREMENTS (SECTION 508)

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 meets some but not all of the standards, the agency must procure the product that best meets the standards.

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

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

(b) The Contractor shall provide, implement, and maintain an IT Security Plan. 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 shall 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 DHS 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.

- In compliance with OMB mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

16.0 IT SECURITY REQUIREMENTS

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 rules and regulations as government employees unless an exception to policy is agreed to by the prime contractors, ICE ISSM and Contracting Officer and detailed in the contract. Non-DHS Federal employees or contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated, whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support contractors and Sub-contractors.

Security Policy References Clause
The following primary DHS/ICE IT Security 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
- DHS 4300A, IT Security Sensitive Systems Handbook
- ICE Directive, IT Security Policy for SBU Systems

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

Clause # 1. Protection of Sensitive 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.

Clause #2. Information Technology Security Program

If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall establish and maintain an IT Security Program. This program shall be consistent with the referenced DHS/ICE IT security policy documents and at a minimum contain and address the following elements:

(a) Handling of DHS/ICE sensitive information and IT resources to include media protection, access control, auditing, network security, and rules of behavior

(b) Certification and Accreditation and FISMA compliance (C&A) of Systems containing, processing or transmitting of DHS/ICE data

(c) Training and Awareness for Contractor personnel

(d) Security Incident Reporting

(e) Contingency Planning

(f) Security Reviews

(g) Contract Closeout Actions

Clause #2a. Handling of Sensitive Information and IT Resources
The Contractor shall protect DHS/ICE sensitive information and all government provided and contractor-owned IT systems used to store or process DHS/ICE sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

(a) Media Protection. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplused, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS/ICE approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, copiers) and the transportation and mailing of sensitive media.)

(b) Access Control. The Contractor shall control user access to DHS/ICE sensitive information based on positive user identification, authentication and authorization (Roles and Rules based) mechanisms. Access control measures employed shall provide protection from unauthorized alternation, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.

(c) **Auditing.** The Contractor shall ensure that its contractor-owned IT systems used to store or process DHS/ICE sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up.

(d) **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between contractor-owned IT systems that process or store DHS/ICE sensitive information and IT systems not controlled by DHS/ICE shall be established through controlled interfaces and documented through formal Interconnection Security Agreements (ISA). The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its email systems are secure, properly configured, and that network protection mechanisms implemented in accordance with DHS/ICE requirements. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems containing DHS/ICE sensitive information to identify security vulnerabilities. The results of this information will be provided to the ICE OCIO for review and to coordinate remediation plans and actions.

(e) DHS employees and contractors shall not transmit sensitive DHS/ICE information to any personal e-mail account that is not authorized to receive it.

(f) **Rules of Behavior.** The Contractor shall develop and enforce Rules of Behavior for contractor-owned IT systems that process or store DHS/ICE sensitive information. These Rules of Behavior must meet or exceed the DHS/ICE rules of behavior.

(g) The Contractor shall adhere to the policy and guidance contained in the DHS/ICE reference documents.

Clause #2b. Training and Awareness

(a) The Contractor shall ensure that all contractor personnel (including subcontractor personnel) who are involved in the management, use, or operation of any IT systems that handle DHS/ICE sensitive information, receive annual training in security awareness, accepted security practices, and system rules of behavior. If the contractor does not use the Ice provided Awareness training, then they must submit to the ISSM their awareness training to the ICE ISSM for approval. Should Contractor Training be approved for use, the contractor will provide proof of training completed to the ICE ISSM when requested.

(b) The Contractor shall ensure that all contractor personnel, including subcontractor personnel, with IT security responsibilities receive specialized DHS/ICE annual

training tailored to their specific security responsibilities. If the contractor does not use the Ice provided Special training, then they must submit to the ISSM their awareness training to the ICE ISSM for approval. Should Contractor Training be approved for use, the contractor will provide proof of training completed to the ICE ISSM when requested.

(c) Any contractor personnel who are appointed as ISSO, Assistant ISSOs, or other position with IT security responsibilities, i.e., System/LAN Database administrators, system analyst and programmers should attend and participate in the DHS Annual Security Conference.

Clause #2c. Certification and Accreditation (C&A) and FISMA compliance
The Contractor shall ensure that any contractor owned systems that process, store, transmit or access DHS/ICE information shall comply with the DHS/ICE C&A and FISMA requirements.
Any work on developing, maintaining or modifying DHS/ICE systems must be done to ensure that DHS/ICE systems are in compliance with the C&A and FISMA requirements. The contractor must ensure that the necessary C&A and FISMA compliance requirements are being effectively meet prior to the System or application is put into Production, to include pilots.
The Contractor shall use the DHS provided tools for C&A and FISMA compliance and reporting requirements.

Clause #2d. Security Incident Reporting
The Contractor shall establish and maintain a computer incident response capability that reports all incidents to the ICE Computer Security Incident Response Center (CSIRC) in accordance with the guidance and procedures contained in the referenced documents.

Clause #2e. Contingency Planning
If performance of the contract requires that DHS/ICE data be stored or processed on Contractor-owned information systems, the Contractor shall develop and maintain contingency plans to be implemented in the event normal operations are disrupted. All contractor personnel involved with contingency planning efforts shall be identified and trained in the procedures and logistics needed to implement these plans. The Contractor shall conduct periodic tests to evaluate the effectiveness of these contingency plans. The plans shall at a minimum address emergency response, backup operations, and post-disaster recovery.

Clause #2f. Security Review and Reporting

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

(b) The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The

Contractor shall afford DHS/ICE, including the Office of Inspector General, ICE ISSM, and other government oversight organizations, access to the Contractor's and subcontractors' facilities, installations, operations, documentation, databases, and personnel used in the performance of this contract. Access shall be provided to the extent necessary for the government to carry out a program of inspection, investigation, and audit to safeguard against threats and hazards to the integrity, availability, and confidentiality of DHS/ICE data or the function of computer systems operated on behalf of DHS/ICE, and to preserve evidence of computer crime.

Clause #2g. Use of Government Equipment
Contractors are not authorized to use government office equipment of IT systems/computers for personal use under any circumstances, unless limited personal use is specifically permitted by the contract. When so authorized, contractors shall be governed by the limited personal use policies in the referenced documents.

Clause #2h. Contract Closeout
At the expiration of this contract, the Contractor shall return all sensitive DHS/ICE information and IT resources provided during the life of this contract. The Contractor shall certify that all DHS/ICE information has been purged from any contractor-owned system used to store or process DHS/ICE information. Electronic media must be sanitized (overwritten or degaussed) in accordance with the sanitation guidance and procedures contained in reference documents and with DHS/NIST/NSA approved hardware and software.

Clause # 3. Personnel Security

(a) DHS/ICE does not permit the use of non U.S. Citizens in the performance of this contract or to access DHS/ICE systems or information

(b) All Contractor personnel (including subcontractor personnel) must have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.

(c) The Contractor shall ensure all contractor personnel are properly submitted for appropriate clearances.

(d) The Contractor shall ensure appropriate controls have been implemented to prevent contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated background investigation has been completed and appropriate clearances have been issued. At the option of the government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this contract by the Contracting Officer.

(e) The Contractor shall ensure its personnel have a validated need to access DHS/ICE sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.

(f) The Contractor shall ensure that its personnel comply with applicable Rules of Behavior for all DHS/ICE and contractor-owned IT systems to which its personnel have been granted access privileges.

(g) The Contractor shall implement procedures to ensure that system access privileges are revoked for contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/ICE sensitive information.

(h) The Contractor shall conduct exit interviews to ensure that contractor personnel who no longer require access to DHS/ICE sensitive information understand their obligation not to discuss or disclose DHS/ICE sensitive information to which they were granted access under this contract.

Clause #4. Physical Security

The Contractor shall ensure that access to contractor buildings, rooms, work areas and spaces, and structures that house DHS/ICE sensitive information or IT systems through which DHS/ICE sensitive information can be accessed, is limited to authorized personnel. The Contractor shall ensure that controls are implemented to deter, detect, monitor, restrict, and regulate access to controlled areas at all times. Controls shall be sufficient to safeguard IT assets and DHS/ICE sensitive information against loss, theft, destruction, accidental damage, hazardous conditions, fire, malicious actions, and natural disasters. Physical security controls shall be implemented in accordance with the policy and guidance contained in the referenced documents.

17.0 CONTRACTOR PERSONNEL SECURITY REQUIREMENTS

17.1 General

The Department of Homeland Security (DHS) has determined that performance of the tasks as described in Contract Independent Verification & Validation Services in Support of the Risk Assessment and Management Program (RAMP) 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.

17.2 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.

17.3 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 45 days before the starting date of the
contract or 45 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. 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"

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.

17.4 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.

17.5 Employment Eligibility

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.

17.6 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.

17.7 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. Contractor 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).

17.8 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).

18.0 CONTRACTOR EMPLOYEE ACCESS (JUNE 2006)

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

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

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

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

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

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

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

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

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

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

(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.

19.0 APPENDIX A: LIST OF ACRONYMS

	Acronym	Description
A		
	AHS	Application Hosting Services
	AJAX	Asynchronous Javascript and XML
B		
	BSA	Building Security Assessment
	BSC	Building Security Committee
C		
	CCB	Change Control Board
	CD	Compact Disk
	CERTS	Contract Employment Requirements Tracking System
	C&A	Certification and Accreditation
	CFR	Code Of Federal Regulation
	CIO	Chief Information Officer
	CLIN	Contract Line Item Numbers
	CO	Contracting Officer
	COTR	Contracting Officer Technical Representative
	COTS	Commercial-Off-The-Shelf
	CSIRC	Computer Security Incident Response Center
D		
	DISCO	Defense Industrial Security Clearance Office
	DHS	Department of Homeland Security
E		
	EA	Enterprise Architecture
	EDMO	Enterprise Data Management Office
	EIS	Enterprise Information System
	EIT	Electronic and Information Technology
	ELMS	Electronic Library Management System
	EOD	Entry on Duty
	EVMS	Earned Value Management System
F		
	FAR	Federal Acquisition Regulation
	FISMA	Federal Information Security Management Act
	FINS	Former Immigration and Naturalization Service operations
	FISTS	FPS Information Support Tracking System
	FPS	Federal Protective Service
	FPSDS	FPS Data System
	FSRM	Federal Security Risk Manager
G		
	GSA	General Services Administration
	GFE	Government Furnished Equipment
	GFI	Government Furnished Information

	Acronym	Description
	GOTS	Government-Off-The-Shelf
H		
	HAZUS	Hazards - US
	HLS EA	Homeland Security Enterprise Architecture
	HQ	Headquarters
I		
	ICE	Immigration and Customs Enforcement
	IDW	Infrastructure Data Warehouse
	IICP	Infrastructure Information Collection Program
	ISC	Interagency Security Committee
	IT	Information Technology
	ISSM	Information Systems Security Manager
	ISSO	Information Systems Security Officer
	IV&V	Independent Verification and Validation
L		
	LPR	Lawful Permanent Residents
M		
	MD	Management Directive
N		
	NIPP	National Infrastructure Protection Plan
	NOAA	National Oceanic and Atmospheric Administration
O		
	OAST	Office on Accessible Systems and Technology
	OCIO	Office of the Chief Information Officer
	ODC	Other Direct Cost
	OISS	Office of Information System Security
	OPR-PSU	Office of Professional Responsibility, Personnel Security Unit
	O&M	Operations and Maintenance
	OMB	Office of Management and Budget
P		
	PA	Privacy Act
	PCII	Protected Critical Infrastructure Information
Q		
	e-QIP	Electronic Questionnaires for Investigation Process
R		
	RAMP	Risk Assessment and Management Program
	RFD	Request For Deviation
S		
	SBU	Sensitive But Unclassified
	SLM	System Lifecycle Management
	SOP	Standard Operating Procedure
	SOW	Statement of Work
	STAR	System for Tracking and Administering Real Property
	STS	Security Tracking System

	Acronym	Description
	SCR	System Change Request
T		
	TM	Task Manager
	TRM	Technology Reference Model
	TTY	Telephone Typewriter
W		
	WebRMS	Web Record Management System
X		
	XML	Extensible Markup Language