

ORDER FOR SUPPLIES OR SERVICES

PAGE OF PAGES

1 8

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

1. DATE OF ORDER 05/23/2008	2. CONTRACT NO. (if any) HSHQDC-06-D-00035	8. SHIP TO: a. NAME OF CONSIGNEE Department of Homeland Security	
3. ORDER NO. HSHQDC-08-J-00117	4. REQUISITION/REFERENCE NO. RCAN-08-00005		

5. ISSUING OFFICE (Address correspondence to) U.S. Dept. of Homeland Security Office of Procurement Operations Information Tech. Acquisition Div. 245 Murray Lane, SW Building 410 Washington DC 20528		b. STREET ADDRESS Citizenship & Immigration Services Chief Information Officer 5th floor #102 111 Massachusetts Ave NW	
		c. CITY Washington	d. STATE DC
		e. ZIP CODE 20001	

7. TO: a. NAME OF CONTRACTOR PRAGMATICS INC		f. SHIP VIA	
b. COMPANY NAME		8. TYPE OF ORDER	
c. STREET ADDRESS 7926 JONES BRANCH DR SUITE 711		<input type="checkbox"/> a. PURCHASE <input checked="" type="checkbox"/> b. DELIVERY	
d. CITY MC LEAN		REFERENCE YOUR: Please furnish the following on the terms and conditions specified on both sides of the order and on the attached sheet, if any, including delivery as indicated.	
e. STATE VA	f. ZIP CODE 221023603	Except for billing instructions on the reverse, this delivery order is subject to instructions contained on this side only of this form and is issued subject to the terms and conditions of the above-numbered contract.	

9. ACCOUNTING AND APPROPRIATION DATA See Schedule		10. REQUISITIONING OFFICE Department of Homeland Security	
--	--	--	--

11. BUSINESS CLASSIFICATION (Check appropriate box(es))				12. F.O.B. POINT Destination	
<input checked="" type="checkbox"/> a. SMALL	<input type="checkbox"/> b. OTHER THAN SMALL	<input type="checkbox"/> c. DISADVANTAGED	<input type="checkbox"/> d. WOMEN-OWNED	<input type="checkbox"/> e. SERVICE-DISABLED VETERAN-OWNED	
<input type="checkbox"/> f. EMERGING SMALL BUSINESS	<input type="checkbox"/> g. HUBZone				

13. PLACE OF		14. GOVERNMENT B/L NO.		15. DELIVER TO F.O.B. POINT ON OR BEFORE (Date) Multiple		16. DISCOUNT TERMS Net 30	
a. INSPECTION Destination	b. ACCEPTANCE Destination						

17. SCHEDULE (See reverse for Rejections)

ITEM NO. (a)	SUPPLIES OR SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	DUNS Number: 153874623+0000 This Time-and-Materials (T&M) task order with firm-fixed-price labor rates and Other Direct Costs/Publishing as cost reimbursable is issued to Pragmatics, Inc. for USCIS OIT Independent Verification and Continued ...					

18. SHIPPING POINT		19. GROSS SHIPPING WEIGHT		20. INVOICE NO.		17(h) TOTAL (Cont. pages)
21. MAIL INVOICE TO:						
a. NAME Department of Homeland Security				\$6,754,730.00		17(i) GRAND TOTAL
b. STREET ADDRESS (or P.O. Box) Departmental Operations Branch Room 3621 245 Murray Lane, SW Building 410						
c. CITY Washington	d. STATE DC	e. ZIP CODE 20528		\$6,754,730.00		

22. UNITED STATES OF AMERICA BY (Signature) (66)		23. NAME (Typed) Joseph Garforth TITLE: CONTRACTING/ORDERING OFFICER	
--	--	--	--

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

2 8

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

DATE OF ORDER
05/23/2008

CONTRACT NO.
HSHQDC-06-D-00035

ORDER NO.
HSHQDC-08-J-00117

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>Validation (IV&V) Support Services in accordance with the attached Statement of Work (Attachment #1) and labor rates/est. labor hours (Attachment #2) for a base period of 12 months and 4 twelve-month option periods ending 5/22/2013. The total estimated value of this task order is (b(4)).</p> <p>Admin Office: Department of Homeland Security Office of Procurement Ops. (ITAC) 245 Murray Drive Bldg. 410 Washington DC 20528</p> <p>Mark For: Department of Homeland Security Office of Procurement Operations 245 Murray Lane Bldg. 410 Washington DC 20528</p>					
0001	<p>USCIS OIT Independent Verification & Validation (IV&V) Support Services Labor in accordance with the attached Statement of Work (SOW). The labor estimated for the Base Year is \$6,681,367.20. This is a T&M CLIN. The period of performance is from 5/23/08 - 5/22/09.</p> <p>Delivery: 30 Days After Receipt of Order</p> <p>Accounting Info: (b(2))</p> <p>Funded: (b(4))</p> <p>Accounting Info: (b(2))</p> <p>Funded: (b(4))</p>				(b(4))	
0002	<p>Travel for CLIN 0001. All travel must be in accordance with the Federal Travel Regulations (FTR) and authorized by the Contracting Officer's Technical Representative (COTR) prior to Continued ...</p>	(b(4))

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES
3 8

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

DATE OF ORDER
05/23/2008

CONTRACT NO.
HSHQDC-06-D-00035

ORDER NO.
HSHQDC-08-J-00117

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>expenditure. The estimated value of (b(4)) is for travel costs that includes the mark-up. Travel costs (b(4)) are cost reimbursable with a (b(4)) (b(4)) for the Base Year. Travel is in support CLIN 0001. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/08 - 5/22/09.</p> <p>Delivery: 05/19/2009 Accounting Info: (b(2))</p> <p>Funded: (b(4))</p>					
0003	<p>Other Direct Costs (ODCs)/Publishing for support of CLIN 0001. The estimated value of (b(4)) is for ODCs/Publishing costs that includes the mark-up. The ODCs/Publishing costs (b(4)) are cost reimbursable including (b(4)) (b(4)) for the Base Year. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/08 - 5/22/09.</p> <p>The total estimated value for the Base Year is \$6,754,730.00 (Ceiling Price). Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p> <p>Accounting Info: (b(2))</p> <p>Funded: (b(4))</p>	(b(4))	
1001	<p>Option Year 1. USCIS OIT Independent Verification & Validation (IV&V) Support Services, in accordance with the attached Statement of Work. The labor estimated for Option Year 1 is (b(4)) This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/09 - 5/22/10. Continued ...</p>	(b(4))	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

4 8

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

DATE OF ORDER
05/23/2008

CONTRACT NO.
HSHQDC-06-D-00035

ORDER NO.
HSHQDC-08-J-00117

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
1002	<p>Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p> <p>Option Year 1 Travel for CLIN 1001. All travel must be in accordance with the Federal Travel Regulations (FTR) and authorized by the Contracting Officer's Technical Representative (COTR) prior to expenditure. The estimated value of (b(4)) is for travel costs that includes the mark-up. (b(4)) (b(4)) are cost reimbursable with a (b(4)) for Option Year 1. This travel is in support of CLIN 1001. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/09 - 5/22/10.</p> <p>Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p>	1	EA	0.00	0.00	
1003	<p>Option Year 1 Other Direct Costs (ODCs)/Publishing for support of CLIN 1001.</p> <p>The estimated value of (b(4)) is for ODCs/Publishing costs that includes the mark-up. The ODCs/Publishing costs (b(4)) are cost reimbursable including a (b(4)) for Option Year 1. This is a Time-and-Materials (T&M) CLIN.</p> <p>The period of performance is from 5/23/09 - 5/22/10.</p> <p>The total estimated value for Option Year 1 is (b(4)) (Ceiling Price).</p> <p>Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p>	1	EA	0.00	0.00	
2001	<p>Option Year 2. USCIS OIT Independent Verification & Validation (IV&V) Support Services, in accordance with the attached Statement of Work (SOW). The labor Continued ...</p>	1	EA	0.00	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

5 8

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

DATE OF ORDER CONTRACT NO.

05/23/2008 HSHQDC-06-D-00035

ORDER NO.

HSHQDC-08-J-00117

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>estimated for Option Year 2 is (b(4)) This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/10 - 5/22/11. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p>					
2002	<p>Option Year 2 Travel for CLIN 2001. All travel must be in accordance with the Federal Travel Regulation (FTR) and authorized by the Contracting Officer's Technical Representative (COTR) prior to expenditure. The estimated value of (b(4)) is for travel costs that includes the mark-up. Travel costs (b(4)) are cost reimbursable with a (b(4)) for Option Year 2. Travel is in support of CLIN 2001. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/10 - 5/22/11. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p>	1	EA	0.00	0.00	
2003	<p>Option Year 2 Other Direct Costs (ODCs)/Publishing for support of CLIN 2001. The estimate of (b(4)) is for ODCs/Publishing costs, that includes the mark-up. The ODCs/Publishing costs (b(4)) are cost reimbursable including a (b(4)) for Option Year 2. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/10 - 5/22/11.</p> <p>The total estimated value for Option Year 2 is (b(4)) (Ceiling Price). Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p>	1	EA	0.00	0.00	
3001	<p>Option Year 3. USCIS OIT Independent Continued ...</p>	1	EA	0.00	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

6 8

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

DATE OF ORDER 05/23/2008	CONTRACT NO. HSHQDC-06-D-00035	ORDER NO. HSHQDC-08-J-00117
-----------------------------	-----------------------------------	--------------------------------

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
3002	<p>Verification & Validation (IV&V) Support Services-, in accordance with the attached Statement of Work (SOW). The labor estimated for Option Year 3 is (b(4)) This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/11 - 5/22/12. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p> <p>Option Year 3 Travel for CLIN 3001. All travel must be in accordance with the Federal Travel Regulations (FTR) and authorized by the Contracting Officer's Technical Representative (COTR) prior to expenditure. The estimated value of (b(4)) is for travel costs that includes the mark-up. Travel costs (b(4)) are cost reimbursable with a (b(4)) for Option Year 3. Travel is in support of CLIN 3001. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/11 - 5/22/12. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p>	1	EA	0.00	0.00	
3003	<p>Option Year 3 Other Direct Costs (ODCs)/Publishing for support of CLIN 3001. The estimate of (b(4)) is for ODCs/Publishing costs that includes the mark-up. The ODCs/Publishing costs (b(4)) are cost reimbursable including a (b(4)) for Option Year 3. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/11 - 5/22/12.</p> <p>The total estimated value for Option Year 3 is (b(4)) (Ceiling Price). Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES Continued ...</p>	1	EA	0.00	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES

7

8

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

DATE OF ORDER
05/23/2008

CONTRACT NO.
HSHQDC-06-D-00035

ORDER NO.
HSHQDC-08-J-00117

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
4001	Option Year 4. USCIS OIT Independent Verification & Validation (IV&V) Support Services, in accordance with the attached Statement of Work (SOW). The labor estimated for Option Year 4 is (b(4)) This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/12 - 5/22/13. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES	1	EA	0.00	0.00	
4002	Option Year 4 Travel for CLIN 4001. All travel must be in accordance with the Federal Travel Regulations (FTR) and authorized by the Contracting Officer's Technical Representative (COTR) prior to expenditure. The estimated value of (b(4)) is for travel costs that includes the mark-up. Travel costs (b(4)) are cost reimbursable with a (b(4)) for Option Year 4. Travel is in support of CLIN 4001. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/12 - 5/22/13. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES	1	EA	0.00	0.00	
4003	Option Year 4 Other Direct Costs (ODCs)/Publishing for support of CLIN 4001. The estimate of (b(4)) is for ODCs/Publishing costs that includes the mark-up. The ODCs/Publishing costs (b(4)) are cost reimbursable including (b(4)) for Option Year 4. This is a Time-and-Materials (T&M) CLIN. The period of performance is from 5/23/12 - 5/22/13. The total estimated value for Option Year 4 is (b(4)) (Ceiling Price) Continued ...	1	EA	0.00	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H))

**ORDER FOR SUPPLIES OR SERVICES
SCHEDULE - CONTINUATION**

PAGE OF PAGES
2 8

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

DATE OF ORDER: 05/23/2008
CONTRACT NO: HSHQDC-06-D-00035

ORDER NO: HSHQDC-06-J-00117

ITEM NO. (A)	SUPPLIES/SERVICES (B)	QUANTITY ORDERED (C)	UNIT (D)	UNIT PRICE (E)	AMOUNT (F)	QUANTITY ACCEPTED (G)
	<p>The Contractor's signature below signifies that they hereby agree to all terms and conditions of this EAGLE task order HSHQDC-06-J-00117, which is issued under their EAGLE Contract No. HSHQDC-06-D-00035.</p> <p><i>Paul Stein</i> <u>5/23/08</u> Signature of Contractor: Date</p> <p>NOTE: The Government reserves the right to firm-fixed-price (FFP) these IV&V task areas identified in the Statement of Work within the period of performance to include any option period exercised. Product/Service Code: D399 Product/Service Description: OTHER ADP & TELECOMMUNICATIONS SERVICES</p> <p>The total amount of award: \$6,754,730.00. The obligation for this award is shown in box 17(i).</p>					

TOTAL CARRIED FORWARD TO 1ST PAGE (FROM 17(i))



**U.S. Citizenship
and Immigration
Services**

**Office of Information Technology
(OIT)**

**Independent Verification and Validation (IV&V)
Technical Services**

Task Order

HSHQDC-08-J-00117

Attachment No. 1

Statement of Work

05 March 2008

1.0 Project: Independent Verification and Validation (IV&V) Technical Services

Independent Verification and Validation (V&V) is a systems engineering discipline which helps an information technology (IT) organization build quality into its planning, development, and provisioning of software and infrastructure. Validation examines the complete application (software, hardware, procedures) to determine that the solution meets the user's needs; verification determines if the application produced at each phase/step of the development/enhancement effort is well engineered. Independent Verification and Validation (IV&V) is a process of monitoring and evaluating applications performed by an organization that is developing the solution. The Contractor shall provide USCIS an IV&V Capability through the monitoring and evaluation of IT governance and projects via activities such as, but not limited to, assessments, process and procedure audits, project and performance management, and systems analysis and design.

2.0 Background: IV&V Capability

The mission of USCIS is *"to secure America's promise as a nation of immigrants by providing accurate and useful information to our customers, granting immigration and citizenship benefits, promoting an awareness and understanding of citizenship, and ensuring the integrity of our immigration system."* The acquisition goal of the USCIS in acquiring an IV&V capability is to secure technical services to ensure USCIS provides quality IT application and infrastructure products using Industry's Best Practices in a cost-effective and cost efficient manner. Currently, USCIS IV&V activities are conducted on IT new development and those products that have already in operation. However, USCIS is interested in expanding the scope and effectiveness of its IV&V services to ensure the provisioning of quality IT products. In acquiring full USCIS Office of Information technology (OIT) IV&V Capability, USCIS will put into place a capability to conduct IV&V activities of its IT solutions from inception to completion.

3.0 Scope: USCIS IV&V Requirements

The Contractor shall provide a proper skill mix and level of personnel resources to provide USCIS an IV&V capability to support the full Information Technology Lifecycle and governance of its IT application and infrastructure solutions. USCIS requires an IV&V Capability that makes use of technical methods and concepts based on Government statutory and regulatory guidelines as well as Industry's Best Practices (Section 4.0). The Contractor shall provide IV&V technical methods, processes, and concepts that are innovative, practical, cost-effective and conducive to an Information Technology Lifecycle quality monitoring environment. The Contractor shall be responsible for providing the proper level of IV&V resources, as required, that are qualified and experienced in the following Information Technology Lifecycle Task Areas:

- Business Management (Section 5.2)
- Evaluate Project Planning (Section 5.3)
- Project Management (Section 5.4)
- Requirements Managements(Section 5.5)

- Quality Assurance(Section 5.6)
- Configuration, Change and Release Management(Section 5.7)
- Training (Section 5.8)
- Operating Environment (Section 5.9)
- Monitoring Software Development (Section 5.10)
- Test and Evaluation (Section 5.11)
- Data Management (Section 5.12)
- IT Security Auditing (Section 5.13)
- Capability Maturity Model Integration (CMMI) (Section 5.14)
- IT Governance and Enterprise Architecture (Section 5.15)
- IV&V Strategic and Management Support (Section 5.16)

4.0 Applicable References: Technical Methods, Concepts and Industry’s Best Practices

The Contractor shall use the following references with regards to the IV&V technical methods, concepts, and Industry’s Best Practices as overarching technical guidance in providing USCIS an IV&V capability. Additionally, within the body of the SOW, there will be reference documents that are not listed in the table below, but contain pertinent information relative to the SOW section in which they are identified. The Contractor shall be responsible for being knowledgeable and familiar with the most current reference guidance. Below reference versions are current as of issuance of the RFQ.

Document Name	Publication Number/Applicable Web Site
DHS Enterprise Architecture	IT Security Architecture Vol 1: Network & Systems Infrastructure
	IT Security Architecture Vol 2: Security Operations and Support
	IT Security Architecture Vol 3: Application Infrastructure Design
USCIS Enterprise Architecture	USCIS Enterprise Architecture
DHS Strategic Plan	http://www.dhs.gov/xabout/strategicplan/
DHS Technical Reference Model	

Document Name	Publication Number/Applicable Web Site
CPIC	Capital Planning and Investment Control (CPIC) Guide
Institute of Electrical and Electronic Engineers Standard for Software Verification and Validation	IEEE Std 1012-2004 ISBN: 0738146412
USCIS OIT Information Technology Lifecycle Management (ITLM)	(b(2)) (b(2)) The ITLM is a USCIS OIT document that shall serve as interim guidance for OIT IT acquisitions until the DHS "System Lifecycle Guide" (SLC) becomes effective. It replaces the current USCIS SDLC Manual. The most current SLC is "draft" Version 0.9 dated 14 December 2007 and is being reviewed internally by DHS and is not available for public dissemination at this time
CCRM	OIT CCRM Process
The Software Engineering Institute (SEI) Capability Maturity Model-Integrated	http://www.sei.cmu.edu/cmmi/ http://www.sei.cmu.edu/cmmi/publications/cmmi-book-v12.html
Standard CMMI Appraisal Method for Process Improvement (SCAMPI)	Method Definition Document CMU/SEI-2006-HB-002
DHS Management Directive (MD) 4300	IT Systems Security
Information Systems Audit and Control Association (ISACA) – Certified Information System Auditor (CISA)	ISO/IEC 17024:2003 http://www.iso.org/iso/en/CatalogueDetailPage.CatalogueDetail?CSNUMBER=29346 http://www.isaca.org/
Control Objectives for Information and related Technology (CoBIT) practices.	ISBN 1-933284-72-2 www.itgi.org
Earned Value Management Systems	American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-1998(R2002)
Information Technology Infrastructure Library (ITIL)	http://www.itil.org.uk/
Information Security Certification & Accreditation Remediation Plan for Information Systems IV&V Project Manager.	http://www.isaca.org/Template.cfm?Section=Home&CONTENTID=20608&TEMPLATE=/ContentManagement/ContentDisplay.cfm
DHS Management Directive (MD) 4010	Section 508 Program Management Office & Electronic and Information Technology Accessibility
Section 508 Compliance	Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220) http://www.section508.gov/index.cfm?fuseAction=Content&ID=12

All of the above references are available for review. The point of contact for access to these documents is Ms. Darcy Bingham (202) 272-8669. The above Government references are for official use only (FOUO) or are DHS sensitive. These documents will be made available for viewing, but shall not leave the DHS library, photocopied, or pen copied verbatim while viewing. All individuals will be monitored by a DHS representative while viewing the documents.

Additional GFI will be provided to the awardee on a "as needed basis" in support of their IV&V activities under this contract

5.0 IV&V Task Area Descriptions

The Contractor shall provide IV&V services over 15 Tasks Areas that covers the Information Technology Lifecycle for IT work products associated with USCIS IT acquisitions. The Contractor shall provide USCIS an IV&V capability by conducting the activities described in each of the individual Task Areas (Sections 5.2 through 5.16). In support of these activities, the contractor shall be responsible for documenting their IV&V efforts via contract deliverables as identified in Section 6.0 of this SOW coordinated through the IV&V COTR.

Additionally, the Contractor shall assist the USCIS OIT IV&V Project Manager in coordinating, monitoring, and managing the overall USCIS OIT IV&V process (See Section 5.16) in conjunction with providing USCIS OIT IV&V services. The IV&V activities conducted by the Contractor shall be in accordance with the description of IT IV&V services under Functional Category 3 (Independent Test, Validation, Verification and Evaluation) as presented in the Enterprise Acquisition Gateway for Leading-Edge Solutions (EAGLE) Ordering Guide

5.1 IV&V Contractor Efforts

The USCIS OIT IV&V COTR shall work with the IV&V Contractor as required with regard to the Contractor's IV&V efforts. All IV&V efforts will be based upon the IV&V activities described in Sections 5.2 through 5.16 of this SOW. The Contractor shall only conduct IV&V activities identified herein as coordinated through the COTR. Additionally, the Contractor shall only disseminate IV&V findings/deliverables (e.g. reports, briefings [oral and written], white papers, and emails,) as communicated by the USCIS OIT IV&V COTR. Additionally, the IV&V Contractor shall immediately notify the USCIS OIT IV&V contracting officer via the COTR of any direction and/or guidance with regards to the Contractor's IV&V efforts outside of what is contained within the scope of this SOW.

5.1.1 Earned Value Management

The Contractor shall provide Earned Value Management reporting in accordance with the guidance provided in Section H.32 of their basic EAGLE contract. The Contractor shall include as part of their monthly invoice (SOW Section 10.0) an Earned Value Management Report.

5.2 Business Management Task Area Description Activities

The Contractor shall conduct IV&V activities related to Business Management to include:

- 5.2.1 Verify and validate that the project office has established and complies with the processes and procedures for receiving, reviewing, accepting, rejecting, disseminating and storing of contract deliverables.
- 5.2.2 Verify that there are processes and procedures for communication between the Government project support staff, the performance Contractor, and the Government Contracting Officer for the project.
- 5.2.3 Verify and validate that there are established processes and procedures for the timely review and approval of invoices and to ensure the Contractor adheres to all contract performance metrics.
- 5.2.4 Verify and validate that the project office is staffed with an adequate number of assigned personnel possessing the required skills and experience to properly manage the contract.
- 5.2.5 Verify and validate that the project office is in compliance with the most current published DHS/USCIS/USCIS Organizational Element (OE) (order of authority policy guidance/directives with regards to business management process and procedures and that any deviation from policy guidance/directives is documented in the form of an approved waiver or mitigation plan.

5.3 Evaluate Project Planning Task Area Activities

The Contractor shall conduct IV&V activities related to Project Planning to include:

- 5.3.1 Verify and validate that the project fully supports and adheres to USCIS and DHS Strategic Objectives. Identify shortfalls and make recommendations to correct any deficiencies.
- 5.3.2 Review and make recommendations to ensure that solicitation documents adequately inform potential vendors about project objectives, requirements, risks, and other solicitation documentation components (example: ensure that legal, regulatory, policy and security references or applicable documentation are current and contain the correct document name, version, and applicable section references).
 - 5.3.2.1 Verify that high-visibility contractual clauses are included within the solicitation documentation and are presented in a manner that can be readily and easily interpreted by the potential vendors. (e.g. Section 508 compliance, Earned Value reporting requirements)
- 5.3.3 Verify and validate that solicitation evaluation criteria are consistent with project objectives evaluation processes and are consistently applied. Verify evaluation criteria are metrics-based and clearly articulated within the solicitation documents and make any recommendations necessary to improve the evaluation criteria.

- 5.3.4 Verify and validate that the obligations of the vendor, sub-contractors and external staff are clearly defined (e.g. terms, conditions, statement of work, requirements, technical standards, performance standards, development milestones, acceptance criteria, delivery dates, etc.). This includes ensuring the inclusion of performance metrics allowing the tracking of project performance and progress against the program's criteria.
- 5.3.5 Perform continuous assessments and reviews of program methodologies used for feasibility studies, ensuring that the methodologies are objective, reasonable, measurable, repeatable, consistent, accurate and verifiable. Review, evaluate, and ensure that Cost Benefit Analyses are reasonable.
- 5.3.6 Verify that all reasonable alternatives for meeting projects needs have been considered. Verify and validate that there are established processes for conducting realistic Market Research and Surveys.
- 5.3.7 Verify and validate the projects risks, costs, and benefits.

5.4 Project Management Task Area Description Activities

The Contractor shall conduct IV&V activities related to Project Management to include:

- 5.4.1 Verify and validate that the project is staffed with an adequate number of assigned personnel possessing the required certifications, qualifications, skills and experience to properly manage the contract.
- 5.4.2 Verify that there are established program control processes to properly manage the project (e.g. Risk Management Planning, internal and external reporting processes and procedures, Earned Value Reporting monitoring, budget monitoring, etc.).
- 5.4.3 Verify and validate that there is a process for communicating between the project management office, the corresponding USCIS business office and IT product end-users.
- 5.4.4 Verify compliance with the established program control processes.

5.5 Requirements Management Task Area Activities

The Contractor shall conduct IV&V activities related to Requirements Management to include:

- 5.5.1 Verify and validate there are established processes and procedures for requirements' management which are articulated in accurate and concise documentation. Verify that there are requirements' tracking tools established and readily available throughout the Information Technology Lifecycle.
- 5.5.2 Make recommendations to the USCIS OE responsible for generating USCIS business and IT system requirements regarding standard framework for the collection, storage and validation of those requirements.

- 5.5.3 Verify and validate that there is a process for managing and coordinating requirements' documentation. Verify that recommended revisions to requirements are conducted in accordance with existing management policies, processes, and procedures.
- 5.5.4 Verify and validate that there is a process in place for establishing and maintaining standard processes for identifying, tracking, and resolving issues related to the business and IT Project requirements.
- 5.5.5 Verify and validate that sufficient amount of training and briefings on industry best practices in the field of business and IT requirements' management exists.
- 5.5.6 Verify and validate that system requirements are well-defined, understood and documented.
- 5.5.7 Verify and validate that there is a process for allocating system requirements to hardware and software requirements.
- 5.5.8 Verify and validate that software requirements can be traced through a Commercial-Off-The-Shelf (COTS) software application's functionality specification, or design code functionality specifications and test phases, to verify that the system performs as intended and contains no unnecessary software elements.
- 5.5.9 Verify that all business and IT requirements are under formal configuration control.
- 5.5.10 Examine the current "as is" condition of operational (legacy) IT systems. This will be used by the Contractor as a basis for further analysis and as a means to gain a clearer understanding of the business processes being supported.
- 5.5.11 Analyze and provide recommendations to establish an integrated enterprise solution meeting the specified functional requirements and in keeping with the USCIS and DHS enterprise architectures as an enterprise-level service in support of the USCIS "Transformation" efforts.
- 5.5.12 Provide transition planning strategy recommendations and actions to achieve the desired "end-state" and all of the estimated costs associated with making the transition.
- 5.5.13 Verify and validate that security concerns are considered during the requirements' phase and are incorporated into the initial design.
- 5.5.14 Verify and validate that recommendations are made on project policies and procedures to ensure that the system is secure and that the privacy of client data is maintained.
- 5.5.15 Evaluate the projects' restrictions on system and data access.
- 5.5.16 Verify and validate that project security and risk analysis are conducted as part of the requirements' generation process.

- 5.5.17 Verify and validate that processes are established to safely back up and archive client and project data at appropriate intervals.
- 5.5.18 Verify and validate that an analysis of client, program and agency needs and objectives have been performed in order to verify that requirements of the system are well understood, well defined, and satisfy Federal statutory and regulatory requirements.
- 5.5.19 Verify and validate that stakeholders have been consulted about the desired functionality of the system, and that users have been involved in the prototyping of the user interface.
- 5.5.20 Verify and validate that stakeholders are consulted and have agreed to changes that impact project objectives, cost, or schedule.
- 5.5.21 Verify and validate that performance requirements (e.g. timing, response time and throughput) satisfy user needs.
- 5.5.22 Verify and validate that the user's maintenance requirements for the system are completely specified.
- 5.5.23 Validate the requirements'-gathering process to ensure accuracy and integrity.
- 5.5.24 Verify and validate that all system interfaces, including input/output control codes, are accurately described, by medium and by function.
- 5.5.25 Verify and validate that approved interface documents are available and that appropriate relationships (such as interface working groups) are established.
- 5.5.26 Verify and validate that all system requirements have been allocated to either a software or hardware subsystem.
- 5.5.27 Verify and validate that requirement specifications have been developed in a sufficient level of detail.

5.6 Quality Assurance Task Area Description Activities

The Contractor shall conduct IV&V activities related to Quality Assurance to include:

- 5.6.1 Verify and validate that all system and infrastructure projects follow the Information Technology Lifecycle Management (ITLM) processes.
- 5.6.2 Develop an ITLM development methodology/work products plan for the projects.
- 5.6.3 Verify and validate the quality of all IT Lifecycle work-products produced by the project
- 5.6.4 Verify that projects are prepared properly and participate in ITLM gate reviews.
- 5.6.5 Verify that projects have received formal approval at gate reviews before entering new phases of the lifecycle.

- 5.6.6 Verify and validate that project self-evaluations are performed and that measures are continually taken to improve the process.
- 5.6.7 Review and make recommendations on all defined processes and product standards associated with the project.
- 5.6.8 Verify and validate that all major development processes are defined and that the defined and approved processes and standards are followed in development.
- 5.6.9 Verify and validate that the processes and standards are compatible with each other and with the system development methodology.

5.7 Configuration, Change and Release Management Task Area Description Activities

The Contractor shall conduct IV&V activities related to Configuration, Change and Release Management to include:

- 5.7.1 Verify and validate that the configuration management identification process is established for software and hardware and documented properly.
- 5.7.2 Verify that all audit changes, deviations, and waivers are tracked and controlled.
- 5.7.3 Verify that configuration audits and reviews are conducted on a routine basis.
- 5.7.4 Verify and validate the enterprise-wide use of Configuration Management (CM) tool suite and ensure that the USCIS CM investments and software assets are maintained.
- 5.7.5 Verify that CM software tools are analyzed and evaluated on a routine basis.
- 5.7.6 Verify that IT products and technical specifications are researched via a well-defined process.
- 5.7.7 Verify that the USCIS Information Technology Document Library and the Tracker Program, which houses all of the USCIS authorized IT documents, approved systems change requests, in-house developed applications, and software are properly managed and maintained
- 5.7.8 Verify that all software and hardware configuration items changes are property tested and that only correct versions of authorized software and hardware are installed in the production environment.
- 5.7.9 Verify that there is an existing process to establish application release categories and enforce standard processes associated with those categories.
- 5.7.10 Verify and validate there is an established process to facilitate the Test Readiness Review (TRR) and Release Readiness Review (RRR) for all USCIS OIT development and release efforts.

- 5.7.11 Verify and validate that there is an established process to administer and manage the content of the USCIS document library, hardware store, and release management communication tools (including posting system releases).
- 5.7.12 Review and evaluate the configuration management (CM) plans and procedures associated with the development process.
- 5.7.13 Verify and validate with the Developer that all critical development documents, including but not limited to requirements, design, and code are maintained under an appropriate level of control.
- 5.7.14 Verify and validate that there are established processes and tools to identify code versions and to rebuild system configurations from source code.
- 5.7.15 Verify that the appropriate source and object libraries are maintained for training, test, and production and that formal sign-off procedures are established for approving deliverables.
- 5.7.16 Verify and validate that appropriate processes and tools are established to manage system changes, including formal logging of change requests and the review, prioritization and timely scheduling of maintenance actions.
- 5.7.17 Verify that mechanisms are established to prevent unauthorized changes from being made to the system and to the wrong version.

5.8 Training Task Area Description Activities

The Contractor shall conduct IV&V activities related to Training to include:

- 5.8.1 Review and make recommendations to improve the training provided to system-users. Verify that there is a sufficient transfer of knowledge for maintenance and operation of the new system.
- 5.8.2 Verify and validate that material and service desk support is easily available to all users.
- 5.8.3 Verify and validate that necessary training policies, processes, and documentation are available to users.
- 5.8.4 Verify and validate that all training is evaluated and monitored for effectiveness.

5.9 Operating Environment Task Area Description Activities

The Contractor shall conduct IV&V activities related to the Operating Environment to include:

- 5.9.1 Evaluate new and existing system hardware configurations to determine if their performance is adequate to meet existing and proposed requirements.

- 5.9.2 Verify whether the hardware is compatible with the existing processing environment, is maintainable, and is easily upgradeable. This evaluation will include, but is not limited to, Central Processing Units (CPUs) and other processors, memory, network connections and bandwidth, communication controllers, telecommunications systems Local Area Networks/Wide Area Networks (LAN/WAN), terminals, printers and storage devices.
- 5.9.3 Evaluate current and projected vendor support of the hardware.
- 5.9.4 Evaluate new and existing system software to determine if its capabilities are adequate to meet existing and proposed system requirements
- 5.9.5 Evaluate whether the software is compatible with the existing hardware and software environment, is maintainable, and is easily upgradeable. This evaluation will include, but is not limited to, operating systems, middleware, and network software including communications and file-sharing protocols.
- 5.9.6 Evaluate current and projected vendor support of the software.
- 5.9.7 Evaluate new and existing database products to determine if their capabilities are adequate to meet existing and proposed system requirements.
- 5.9.8 Verify whether the database's data format is easily convertible to other formats, it supports the addition of new data items, it is scaleable, it is easily refreshable and it is compatible with the database's existing hardware and software.
- 5.9.9 Evaluate any current and projected vendor support, as well as USCIS' acquisition plans and procedures.
- 5.9.10 Evaluate the existing processing capacity of the system and verify that it is adequate for current wide needs for both batch and on-line processing.
- 5.9.11 Evaluate the historic availability and reliability of the system including the frequency and criticality of system failure.
- 5.9.12 Evaluate existing measurement and capacity planning programs and evaluate the system's capacity to support future growth.
- 5.9.13 Evaluate the results of any volume testing or stress testing.
- 5.9.14 Make recommendations on changes in processing hardware, storage, network systems, operating systems, COTS software, and software design to meet future growth and improve system performance.
- 5.9.15 Provide simulation and modeling services to ensure USCIS has the means of evaluating parameters before making a high-dollar commitment and impacting the current architecture

5.10 Monitoring Software Development Task Area Description Activities

The Contractor shall conduct IV&V activities related to the Software Development Monitoring to include:

- 5.10.1 Evaluate and make recommendations on existing high level design products to verify that the design is workable, efficient, and satisfies all system and system interface requirements.
- 5.10.2 Evaluate the design products for adherence to the project design methodology and standards.
- 5.10.3 Evaluate the design and analysis process used to develop the design and make recommendations for improvements.
- 5.10.4 Verify and validate that all design products are under configuration control and formally approved before detailed design begins.
- 5.10.5 Evaluate and make recommendations on existing detailed design products to verify that the design is workable, efficient, and satisfies all high level design requirements.
- 5.10.6 Evaluate the design products for adherence to the project design methodology and standards.
- 5.10.7 Verify and validate that design requirements can be traced back to system requirements and high level design.
- 5.10.8 Verify and validate that all design products are under configuration control and formally approved before coding begins.

5.11 Test and Evaluation Task Area Description Activities

The Contractor shall conduct IV&V activities related to the Test and Evaluation to include:

- 5.11.1 Evaluate the plans, requirements, environment, tools, and procedures used for integration testing of system modules.
- 5.11.2 Evaluate the level of automation and the availability of the system test environment.
- 5.11.3 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, including formal logging of errors found in testing.
- 5.11.4 Evaluate the plans, requirements, environment, tools, and procedures for pilot testing the system.

- 5.11.5 Verify that a sufficient number and type of case scenarios are used to ensure that a comprehensive, but manageable, testing is run in a realistic and real-time environment.
- 5.11.6 Verify that test scripts are complete, with step-by-step procedures, required pre-existing events or triggers, and expected results.
- 5.11.7 Verify that test results are verified, that the correct code configuration has been used, and that the tests runs are appropriately documented, including formal logging of errors found in testing.
- 5.11.8 Evaluate interface testing plans and procedures for compliance with industry standards and Federal Statutory and Regulatory guidance applicable to USCIS IT investments (e.g. 1998 Amendment to Section 508 of the Rehabilitation Act (29 US Code 794d) as amended by the Workforce Improvement Act of 1998 P.L. 105-220 dated 7 August 1998.
- 5.11.9 Verify how acceptance procedures and acceptance criteria for each product must be defined, reviewed, and approved prior to testing and how the results of the test must be documented. Acceptance procedures must also address the process to correct any software product which fails acceptance testing.
- 5.11.10 Verify the satisfactory performance of the appropriate acceptance testing based on the defined acceptance criteria before software products are accepted.
- 5.11.11 Provide Integrated Performance and Security Testing and documentation on new and modified system in accordance with the applicable procedures and processes within the documents identified in Section 4.0 of this SOW. This testing will ensure that the IT product/s delivered to the field will perform the required functions within performance requirements in a secure fashion within the existing infrastructure. It is imperative that IV&V of this nature be performed in consideration of all IT components and processes necessary to deliver service to the end user.
- 5.11.12 Provide load and stress testing and interpret results to determine application response times for discrete transactions. The Contractor shall verify activities are coordinated with all stakeholders according to schedules and plans, while ensuring testing activities are thoroughly documented in support of lifecycle development activities.
- 5.11.13 Provide System Acceptance Testing (SAT) services to assess whether the final product meets the approved requirements and design specifications. The Contractor shall use the functional requirements as described in the Functional Requirements Document to determine if the product performs the business functions as needed by the user.
- 5.11.14 Develop a SAT plan for each USCIS application and provide daily electronic SAT status report.
- 5.11.15 Provide a final independent SAT Analysis Summary Report.

- 5.11.16 Develop a standard User Acceptance Testing (UAT) template and instruction sheet.
- 5.11.17 Support UAT facilitation activities to include: identifying, tracking and reporting all defects and discrepancies; providing management with daily and weekly status reports; and compiling a UAT Test Analysis Summary Report.
- 5.11.18 Provide Security testing services to validate how well a system meets predefined technical control security requirements to prevent unauthorized internal or external access or willful damage. The Contractor shall conduct Security testing to establish an application's security baseline and identify a level of security risk prior to production implementation.
- 5.11.19 Support USCIS in setting up a virtual lab service, to be provisioned by the USCIS OIT TEC Center that is a configuration-controlled environment with production matched (or production-like) equipment and software. The lab service should be agile in its ability to configure and/or reallocate shared resources according to an aggressive schedule. The Contractor shall specify test environments and administer virtual lab environments assigned by the TEC Center team to provide support of USCIS lab services in support of: Systems Acceptance Testing, System Security Testing, Interoperability Testing, Performance Testing, Simulation and Modeling, and Application Tuning.
- 5.11.20 Evaluate the plans, requirements, environment, tools, and procedures used for unit testing system modules.
- 5.11.21 Provide Section 508 compliance testing.

5.12 Data Management Task Area Description Activities

The Contractor shall conduct IV&V activities related to the Data Management to include:

- 5.12.1 Evaluate existing and proposed plans, procedures and software for data conversion.
- 5.12.2 Verify that procedures are established and followed to review the final data for completeness and accuracy and to perform data clean-up as required.
- 5.12.3 Verify conversion error rates and if the error rates are manageable.
- 5.12.4 Make recommendations to increase the efficiency of the conversion process and to maintain the integrity of the data during the conversion.
- 5.12.5 Evaluate new and existing database designs to determine if they meet existing and proposed system requirements.

- 5.12.6 Recommend improvements to existing designs in order to improve data integrity and system performance.
- 5.12.7 Evaluate the design for maintainability, scalability, refreshability, concurrence, normalization (where appropriate) and any other factors affecting performance and data integrity.
- 5.12.8 Evaluate the project's process for administering the database, including backup, recovery, performance analysis and control of data item creation.
- 5.12.9 Verify the existence and completeness of database design documents, including, but not limited to: Entity Relation Diagram (or equivalent), data dictionary, and database schema.
- 5.12.10 Verify that the database design documents are consistent with what has been deployed.
- 5.12.11 Verify that data entities are mapped to business processes in the detailed design document.

5.13 IT Security Auditing Task Area Descriptions

The Contractor shall conduct IV&V activities related to the IT Security Auditing to include:

- 5.13.1 Provide project planning and scheduling support for all Certification and Accreditation (C&A) activities in accordance with the applicable procedures and processes within the documents identified in Section 4.0 of this SOW.

The Contractor shall provide personnel that possess the following professional certifications to support the activities in this as well as other Task Areas.

- Certified Information Security Manager (CISM)
- Certified Information Systems Auditor (CISA)

- 5.13.2 Provide staff that will travel to USCIS sites (domestically and USCIS international facilities) to perform Certification and Accreditation (C&A) activities. The contractor staff shall have the necessary training, experience, and certifications (examples: Certified Information Systems Security Professional [CISSP], Certified Information Systems Auditor [CISA], Certified Information Systems Manager [CISM] in performing C&A in accordance with Federal Information Management Act (FISMA) of 2002 requirements to include the use of Enterprise C&A Tool, and SecureInfo's Risk Management System (RMS). Typically, the contractor staff will be responsible for all phases of the C&A, to include: Initiation Phase, Security Certification phase, Security Accreditation phase, and Continuous Monitoring phase. Each phase in the C&A process consists of a set of well-defined tasks and subtasks that are to be carried out.

- 5.13.3 As a result of on site C&A activities, the Contractor shall complete the C&A package as a deliverable to the USCIS Information System Security Manager (ISSM) for each site, or system completed in performance of this task order. The C&A shall be packaged with all documents properly loaded into the RMS tool, all documents uploaded into Trusted Agent FISMA (TAF) and accepted by DHS document review staff and finally a Plan of Action and Milestones (POA&M) for deficiencies and entered into TAF.
- 5.13.4 Provide certified staff with experience performing C&A activities in accordance with the DHS Information Security Certification & Accreditation Remediation Plan, Version 1.0, dated September 30, 2005 for Information Systems IV&V Project Manager.
- 5.13.5 As part of the certification and accreditation phases, the Contractor shall prepare a comprehensive assessment of the management, operational, and technical security controls of the information system. This assessment will support the accreditation and will document the extent to which controls are implemented correctly, operating as intended and produce the desired outcomes to meet the DHS/CIS security requirements of the systems.
- 5.13.6 The Contractor shall create Security Assessment Reports (SAR), as required, containing all of the relevant security certification documentation information. Each SAR shall summarize each system evaluation to include an assessment of the adequacy of the system security documentation relating to System Security Plan and Risk Assessment and any testing, inspections and interviews with key system personnel. The SAR shall also summarize the results of the security test and evaluations and includes results of network scans. The SAR shall also outline all the FIPS 199 System Categorizations, ascertain the overall level of risk to the system, document all unmet security requirements, identify all residual risk, and outlines and include a POA&M for mitigation of unmet security requirements.
- 5.13.6.1 The SAR is used as the basis for the Certification Official (CO) to make a recommendation to grant an Authority to Operate (ATO). This recommendation is documented in the CO Letter. The CO Letter notes the FISP 199 Categorization and the level of risk as to Low, Moderate or High. It also categorizes all unmet security requirements, and recommends whether the Designated Accrediting Authority (DAA) should grant an ATO with a suggested time period based upon the system status. An ATO may be granted for up to 3 years.
- 5.13.7 In preparation for the briefing to the DAA, the Contractor shall assist in composing a draft DAA letter. The DAA letter will identify any residual risks. The DAA letter is the official management decision given by a senior agency official to authorize the operation of the system and to explicitly accept the risk to agency operations, agency assets, or individuals based upon the implementation of the security controls.

- 5.13.8 The Contractor shall conduct network scans. As part of the Security Test and Evaluation (STE) of a General Support System, network scans are conducted to support the C&A process. Network tools, the ISS Internet Scanner, and the Microsoft Baseline Analyzer, are used to gather and analyze data to verify and validate the secure operating environments. These tools analyze configurations, patch levels and operating systems to find vulnerabilities related to workstations, servers, and firewalls that could be exploited by hackers. The results of scans are incorporated into the Security Assessment Report.
- 5.13.9 The Contractor shall conduct a Privacy Threshold Analysis (PTA). As part of the Remediation 2006, 11 artifacts (See Section 5.13.9.3) are required for C&A. The PTA is one of these required artifacts and it will be completed for each application or General Support System (GSS). Once entered into the Trusted Agent FISMA (TAF) enterprise management application, the DHS Privacy Office validates the PTA and makes the official determination if a Privacy Impact Assessment (PIA) is needed. Since the Privacy Act relates to major applications that contain systems of records, we anticipate that there will be no Privacy Impact Assessment (PIA) needed for GS Systems. In support of the PTA, the Contractor shall conduct Information Systems Security Office (ISSO) activities as delineated in DHS Management Directive 4300 and Sections 5.13.9.1 through Sections 5.13.9.1 of this SOW.
- 5.13.9.1 The TAF is a DHS enterprise C&A management tool. Both ISSO and security engineers use the TAF to review documents and upload all final C&A documents (currently 11 artifacts). Once uploaded, these artifacts are validated by the appropriate DHS independent verifier and, once approved, count toward 100% goal for each system accreditation. The Contractor shall be responsible for uploading all of the requisite USCIS OIT C&A data into the TAF.
- 5.13.9.2 NIST 800- 53 Controls were required to be implemented no later than March 2007. The current RMS tool incorporates these controls based upon the impact level (high, moderate, low) to each security objective (confidentiality, integrity, and availability) and each GSS is evaluated based upon these security controls. The Contractor shall be responsible for uploading all of the requisite USCIS OIT C&A data into the RMS

5.13.9.3 The Contractor shall prepare C&A Packages. A completed C&A package will typically include the items specified in the following table to comply with established RMS and FISMA standards.

	C&A Document Artifacts
1	FIPS 199 Categorization Completed
2	Privacy Impact Determination/Assessment
3	E-Authentication Determination/Assessment
4	Risk Assessment
5	System Security Plan
6	Contingency Plan
7	Contingency Plan Test Results
8	Security Test & Evaluation Plan
9	Security Assessment Report
10	ATO Letter
11	Annual Self Assessment

5.14 Capability Maturity Model Integration (CMMI) Task Area Description Activities

The Contractor shall conduct IV&V activities related to the CMMI to include:

5.14.1 Perform Standard CMMI Appraisal Method for Process Improvements (SCAMPI) "A" appraisals in accordance with guidelines set forth in the Carnegie Mellon Software Engineering Institute (SEI) "*SCAMPI A Version 1.2 Method Definition Document*" for USCIS IT potential and selected USCIS contractors.

5.14.1.1 The Contractor shall provide personnel that possess the following professional certification to support the activities in this Task Area.

- SEI-SCAMPI Authorized Lead Appraiser

5.14.2 Perform Standard CMMI Appraisal Method for Process Improvements (SCAMPI) "A" High Maturity appraisals in accordance with guidelines set forth in the Carnegie Mellon Software Engineering Institute (SEI) "*SCAMPI A Version 1.2 Method Definition Document*" for USCIS IT potential and selected USCIS contractors.

5.14.2.1 The Contractor shall provide personnel that possess the following professional certification to support the activities in this Task Area.

- SEI-SCAMPI High Maturity Lead Appraiser

5.15 IT Governance and Enterprise Architecture Task Area Description Activities

The Contractor shall conduct IV&V activities related to the IT Governance and Enterprise Architecture to include:

- 5.15.1 Verify and validate that USCIS IT operations and solutions are in strategic alignment and compliance with all DHS/USCIS IT Governance goals, policies and procedures.
- 5.15.2 Verify and validate that USCIS IT solutions are designed, developed, deployed, and operationally maintained in strategic alignment and architectural compliance with all DHS/USCIS IT Enterprise Architectural goals, policies, and procedures.

5.16 IV&V Strategic and Management Support

The Contractor shall provide IV&V Strategic and Management Support to include:

- 5.16.1 Formal Presentations: Prepare and deliver a formal presentation(s) on the status of the USCIS OIT IV&V activities and efforts. USCIS will attempt to provide the Contractor with at least ten (10) business days notice prior to any formal presentation requirements. It is anticipated that there will be no more than one formal presentation per quarter.
- 5.16.1.1 Monthly Status Reports: The Contractor shall provide a monthly report on the status, findings, and recommendations of the individual IV&V activities.
- 5.16.2 The Contractor shall assist the Project Manager in defining the intent and focus of the Contract's IV&V efforts and in coordinating, monitoring, and tracking of all IV&V activities.
- 5.16.3 The Contractor shall develop an IV&V management methodology for the Government.
- 5.16.4 The Contractor shall develop and provide educational and stakeholder briefings on the IV&V, ITLM, and associate processes and procedures training and assistance to USCIS project teams and staff.
- 5.16.5 The Contractor shall support USCIS with the continuous implementation of best practices in the field of IV&V.

6.0 Deliverables and Delivery Schedule

The Government will have 5 business days after receipt of a deliverable to accept or reject any deliverable. If the COTR rejects a deliverable, the Contractor will be provided specific written comments detailing the basis for rejection and the corrective action required. The Contractor shall have 5 business days to address comments by either incorporating the requested Government change or providing an explanation of why the Government requested change is not being incorporated. When responding to Government comments, the Contractor shall respond to the Government with a response for each comment, one copy with tracked changes, and one copy without. Once the Contractor completes this action, the Government will have an additional five business days to review and approve the deliverable.

The Contractor shall deliver all items in a format compatible with Microsoft Office 2003 and accepted by the Government, coordinated via the COTR. Documents submitted by the Contractor shall be professional in content and presentation according to commonly accepted standards of writing and editing in the subject field. All final deliverable documents submitted by the contractor shall meet professional standards. All documents shall be delivered in a format mutually agreed to between the Contractor and the Government. Previously released documentation will be delivered in current format unless mutually agreed otherwise. Multiple document deliverables content may be combined into one delivered document with notification.

	Deliverables	Description	Due Dates	Special Notes
General TO Requirements	<ul style="list-style-type: none"> Kick Off Meeting Presentation 	Power Point Presentation	TO Kick Off meeting	The TO Kickoff Meeting will take place NLT 5 business days after TO award at USCIS OIT HQ. 12 hard copies and 1 soft copy
	<ul style="list-style-type: none"> IV&V Activity Reports 	Each IV&V effort will include a final report documenting all of the findings identified over the course of the Contractor's IV&V activities and will include recommendations regarding any issues identified.	As required and coordinated through the USCIS OIT IV&V COTR	All Contractor IV&V efforts shall not be considered complete until all of the deliverables have been accepted and approved by the government. 2 hard copies and 1 soft copy
	<ul style="list-style-type: none"> Monthly Status Reports 	The Contractor shall provide a monthly status report documenting the status of all ongoing efforts/activities and identifying any issues related to their overall IV&V effort.	30 Days after Contract award and monthly thereafter	2 hard copies and 1 soft copy
	<ul style="list-style-type: none"> Ad Hoc Reporting 	Periodically, there will be a requirement for an Ad Hoc Report during the course of the TO.	As required and coordinated through the USCIS OIT IV&V COTR	The format of the AD Hoc report will be specified IAW the guidance provided by the USCIS OIT IV&V Project Manager/COTR. AD Hoc Reporting is not limited to white papers, Trip Reports, Power Point Presentations, or Spread sheet presentations
In addition to the above general deliverable requirements, each Contractor IV&V efforts (Task Area) shall have deliverable requirements associated with the TASK Area under which the IV&V is taking place. The COTR will include as part of each IV&V specific deliverable requirements that are based on the following but tailored to the needs of the individual IV&V effort.				
Section 5.2	<ul style="list-style-type: none"> IV&V Activity Reports Ad Hoc Report 	Business Management	As required and coordinated through the USCIS OIT IV&V COTR	See Ad Hoc Reporting
Section 5.3	<ul style="list-style-type: none"> IV&V Activity Reports Ad Hoc Report 	Evaluate Project Planning		See Ad Hoc Reporting
Section 5.4	<ul style="list-style-type: none"> IV&V Activity Reports 	Project Management		See Ad Hoc Reporting

	Deliverables	Description	Due Dates	Special Notes
	<ul style="list-style-type: none"> • Ad Hoc Report 		As required and coordinated through the USCIS OIT IV&V COTR	
Section 5.5	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	Requirements Management		See Ad Hoc Reporting
Section 5.6	<ul style="list-style-type: none"> • IV&V Activity Reports • Work Product Plan • Ad Hoc Report 	Quality Assurance		See Ad Hoc Reporting
Section 5.7	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	CCRM		See Ad Hoc Reporting
Section 5.8	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	Training Reports		See Ad Hoc Reporting
Section 5.9	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	Operating Environment		See Ad Hoc Reporting
Section 5.10	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	Monitoring Software Development		See Ad Hoc Reporting
Section 5.11	<ul style="list-style-type: none"> • SAT Plan • SAT Analysis Summary Report • UAT Template • Security Resting Report • TEC C Recommended Configuration Report • Ad Hoc Reporting 	Test and Evaluation		See Ad Hoc Reporting. Reporting formats shall be tailored IAW with guidance provided with the applicable documents identified in Section 4.0 of the this SOW.
Section 5.12	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	Data Management		See Ad Hoc Reporting

	Deliverables	Description	Due Dates	Special Notes
Section 5.13	<ul style="list-style-type: none"> • Project Planning and Scheduling Report for all IV&Vs requiring a C&A effort • C&A Assessment Report • SAR Report • DAA Letter (Draft) • PTA • Ad Hoc Reporting 	IT Security		<p>See Ad Hoc Reporting</p> <p>A Plan of Action and Milestones (POA&M) for deficiencies and entered into TAF.</p> <p>Reporting formats shall be tailored IAW with guidance provided with the applicable documents identified in Section 4.0 of the this SOW.</p>
	<ul style="list-style-type: none"> • C&A Package 			As stipulated with Section 5.13.9.3 of the SOW
Section 5.14	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	CMMI		See Ad Hoc Reporting
Section 5.15	<ul style="list-style-type: none"> • IV&V Activity Reports • Ad Hoc Report 	IT Governance		See Ad Hoc Reporting
Section 5.16	<ul style="list-style-type: none"> • Develop IV&V guidance • IV&V management methodology document • Update USCIS ITLM • ITLM Briefings • Ad Hoc Reporting 	PM Monitoring and Management	As required and coordinated through the USCIS OIT IV&V COTR	See Ad Hoc Reporting

Notes

N1 - All deliverable will be sent to the COTR at USCIS OIT HQ located at 111 Massachusetts Avenue, N.W. Washington D.C. 20536-2001.

The number of hard and soft copies shall be determined by the COTR for all Ad Hoc reporting.

The Contracting Officer shall receive one of the two hard copies of the Monthly Status Report.

7.0 Government Furnished Property (GFP)

The Government shall provide GFP (e.g. GFI) in accordance with Section H.8 of the Contractor's basic EAGLE contract and FAR 52.245-1 Government Property and FAR 52.245-5,

Government Property (Cost-Reimbursement, Time-and-Material, or Labor-Hour Contracts). Specifically, the Government shall provide the following:

- a. GFI: See SOW Section 4.0 for pre-award GFI. For post-award GFI; the IV&V COTR will coordinate with the Contractor to provide any additionally required GFI.
- b. GFE: The Government will provide the Contractor connectivity to the DHS network. The Government will deliver to the Contractor within 10 days of award the following GFE:
 - 50 Desktops will be delivered to the contractor's facility

Government furnished computers will be bar coded for accountability and issued to authorized contractor personnel, who have been cleared through USCIS Security and have signed the DHS consent statement on individual security responsibilities. Each Government Furnished computer is issued for authorized and official government support to this task order. The computers will be configured and no changes, alterations or additional software, or passwords should be programmed.

DHS network connectivity can be accomplished using Government-issued computers, which comply with DHS encryption and PKI requirements. During the performance of this order, the COTR, Property Specialist or Security Specialist may inspect the desktops. At the conclusion of the task order the computers will be returned to the COTR. The Contractor is responsible for any damage, miss use or missing computers. All computers shall be accounted for at all times. Any missing computers shall be reported immediately to the C.O. and COTR!

8.0 Place of Performance

The Contractor will provide Off-site (Contractor facility) services primarily within a fifty (50) mile radius of the Washington DC Metropolitan Area (WMA). Occasionally, the contractor may be required to provide IV&V support at Government facilities as a result of provisions identified within the contractors' DD Form 254.

The Contractor may be required to support a portion of the USCIS IV&V effort outside the Washington Metropolitan Area to include international locations. All travel will comply with Section H6.1 of their Basic EAGLE contract. Work shall be performed for delivery to DHS/USCIS Headquarters (HQ), 111 Massachusetts Ave, N.W., Washington, D.C. 20259.

9.0 Period of Performance

Base and Option Periods

Performance Period	Duration	Start Date/End Date
Base Period	12 months	5/23/08 – 5/22/09
Option Period 1	12 months	5/23/09 – 5/22/10

Option Period 2	12 months	5/23/10 – 5/22/11
Option Period 3	12 months	5/23/11 – 5/22/12
Option Period 4	12 months	5/23/12 – 5/22/13

10.0 Invoicing Procedures

All invoices and requisite supporting invoice documentation shall comply with Section G 6.2 of the Contractor's Basic Eagle Contract) and shall be submitted on a monthly basis electronically to the following Email addresses:

oitinvoice@dhs.gov

IV&V COTR (Email address to be provided at the TO Kick Off meeting)

The Contractor shall be required to provide the Government invoices on a monthly basis (NLT 30 calendar days after the work has been performed). In the event the Contractor is unable to provide a timely invoice; they shall provide in writing the COTR the reason for why the invoice was not provided to the Government in the time specified.

Each invoice in addition to Section G 6.2 of the Contractor's Basic Eagle Contract will provide the following supporting invoice documentation: Costs by Organizational Element (OE) undergoing the IV&V effort by Task Area

- Labor
 - Labor Hours
 - Labor Category
- ODCs
 - Travel
 - Publishing
- Earned Value Management Report (See SOW Section 5.1.1)
- Monthly Status Report (See SOW Section 6.0)

11.0 Organizational Conflict Of Interest (OCOI)

This acquisition may give rise to a potential organizational conflict of interest. The nature of this conflict is based on the premise that the Contractor who provides USCIS OIT IV&V technical services will be granted detailed and in depth access to the programmatic and technical aspects of all USCIS IT acquisitions throughout their IT Lifecycles. The net effect of this in depth access could potentially create a USCIS IT acquisition environment that would afford the USCIS OIT IV&V Contractor an unfair competitive advantage with regards to USCIS IT acquisitions. In order to pre-empt any potential OCOI issues, all Contractors submitting proposals shall be subject to the following:

11.1 OCOI Contractor Proposal Restrictions

The Contractor either as a prime **or a subcontractor [all tiers]** shall adhere to the guidance provided under HSAR 3052.209-72 and within Section H.33 of their Basic EAGLE Contract.

The Contractor and subcontractor [all tiers] awarded the USCIS OIT IV&V Technical Services TO shall be prohibited (other than IV&V efforts) from soliciting, proposing, or being awarded any of the following efforts related to USCIS IT Programs, Projects and/or Services while performing under this TO:

- Project Management

- Requirements Development/Management
- Quality Assurance
- Software/Hardware (including activities related to using Commercial-Off-the Shelf [COTS] IT products) design, development or other manner of implementation phase work.
- IT System design, development, integration, or deployment
- Operations and Maintenance

11.1.1 OCOI Mitigation/Waivers

All proposing Contractors requesting OCOI Mitigation/Waivers should do so in accordance with Section H.33 of their Basic Eagle Contract and included as part of their USCIS OIT IV&V Technical Services proposal. Embedded within the OCOI Mitigation Plan or Waiver Request should be a listing of all Contractor contractual relationships with USCIS as either a Prime or Subcontractor.

12.0 Certification and Credentialing Requirements

The Contractor shall provide IV&V personnel resources that are professionally and technically qualified to conduct the IV&V activities identified within the fifteen (15) Task Areas in Sections 5.2 through 5.16 of this SOW (The Contractor shall pay particular attention to the Certification requirements under Sections 5.13 and 5.14. of this SOW). The Contractor shall provide the COTR the name and certification/credentialing level of all IV&V personnel assigned to conduct IV&V activities prior to commencing their IV&V activities.

12.1 Key Personnel

Key Personnel under this Task Order include the following positions: IV&V Program Manager; IV&V Strategic Management Task Area Lead; SEI SCAMPI Authorized Lead Appraiser; SEI SCAMPI High Maturity Lead Appraiser; Certified Information Security Manager; and Certified Information Systems Auditor. The Government will review resumes. All key personnel shall be assigned full-time to the program.

Key personnel shall be available to support the requirements of the task orders and ensure that all work performed meets the requirements set forth in this Task Order. Key Personnel shall have sufficient experience in the task being performed.

12.2 Substitution or Diversion of Key Personnel

The Contractor shall notify the TO CO and the TO COTR prior to making any changes in Task Order Key Personnel. No changes in TO Key Personnel will be made unless the Contractor can demonstrate that the qualifications of prospective replacement personnel are equal to or better than the qualifications of the TO Key Personnel being replaced. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The TO CO shall be notified in writing of any proposed substitution at least fifteen (15) days, or

thirty (30) days if a security clearance is to be obtained, in advance of the proposed substitution. Such notification shall include:

- (a) an explanation of the circumstances necessitating the substitution;
- (b) a complete resume of the proposed substitute; and
- (c) any other information requested by the TO CO to enable him/her to judge whether or not the Contractor is maintaining the same high quality of personnel that provided the partial basis for award.

The EAGLE Program Manager and the contract level CO will evaluate substitutions at the contract level and the TO COTR will evaluate TO level substitutions. These individuals will evaluate such requests and promptly notify the Contractor of his/her approval or disapproval in writing. All disapprovals will require resubmission of another substitution within 15 calendar days by the Contractor.

In the event that a change in key personnel is caused by an individual's sudden illness, death, or termination of employment, the Contractor shall promptly notify the Contracting Officer and provide the information required.

13.0 Points of Contact Mailing Addresses

Contracting Personnel

Joseph M. Garforth Jr. (DHS OPO ITAC): Contracting Officer

245 Murray Drive

Building 410

Washington D.C. 20528

(202) 447-(b(2)) phone

(b(2) b(6))

(b(6)) (DHS OPO ITAC): Contract Specialist

245 Murray Drive

Building 410

Washington D.C. 20528

(b(2) b(6))

Program Manager

(b(6)) (Program Manager)

DHS/USCIS/OIT

111 Massachusetts Avenue, N.W.

Washington, D.C. 20536-2001

(202) 272-(b(2)) Phone

(b(2) b(6))

Project Manager

(b(6))

DHS/USCIS/OIT

111 Massachusetts Avenue, N.W.

Washington, D.C. 20536-2001

(202) 272 (b(2)) 'hone

(b(2) b(6))

COTR

(b(6))

DHS/USCIS/OIT

111 Massachusetts Avenue, N.W.

Washington. D.C. 20536-2001

(202) 272 (b(2)) Phone

(b(2) b(6))

14.0 Information Technology Accessibility Requirements (Section 508)

In accordance with H.27 of the Basic Eagle Contract, all services and Electronic Information Technology (EIT) delivered as result of orders placed under this contract shall comply with accessibility standards in accordance with Federal Information Technology Accessibility as required by Section 508 of the Rehabilitation Act (29 U.S.C. 794d), as amended by the Workforce Investment Act of 1998 (P.L. 105-220). Information about the Section 508 Electronic and Information Technology Accessibility Standards may be obtained via the Web at the following URL: www.Section508.gov.

Section 508 of the Rehabilitation Act 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.

36 CFR 1194.25 – Self Contained, Closed Products, applies to all EIT products such as printers, copiers, fax machines, kiosks, etc. that are procured or developed under this work statement.

36 CFR 1194.26 – Desktop and Portable Computers, applies to all desktop and portable computers, including but not limited to laptops and personal data assistants (PDA) that are procured or developed 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 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 and 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.

15.0 Security Requirements

U.S. Citizenship & Immigration Services (USCIS) has determined that performance of this contract requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), requires access to classified National Security Information (herein known as classified information). Classified information is Government information which requires protection in accordance with Executive Order 12958, Classified National Security Information, and supplementing directives.

The Contractor will abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the contract, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at a USCIS or other Government Facility, it will abide by the requirements set by the agency.

It is anticipated that the vast majority of the work will encompass sensitive, but unclassified systems. However, a small percentage of the work may require access to information classified up to the Top Secret level. An example of such information is some of the programs in the National Security and Records Verification Directorate.

15.1 Suitability Determination

USCIS shall have and exercise full control over granting, denying, withholding or terminating access of unescorted Contractor employees to government facilities and/or access of Contractor employees to sensitive but unclassified information, based upon the results of a background investigation. USCIS 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 USCIS, at any time during the term of the contract. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Office of Security & Investigations (OSI).

15.2 Background Investigations

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the contract, needing access to sensitive but unclassified information, shall undergo a position sensitivity analysis based on the duties, outlined in the Position Designation Determination (PDD) for Contractor Personnel, each individual will perform on the contract. The results of the position sensitivity analysis shall identify the appropriate background

investigation to be conducted. All background investigations will be processed through OSI. Prospective Contractor employees shall submit the following completed forms to OSI through the COTR no less than 30 days before the starting date of the contract or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions"
2. DHS Form 11000-6, "Conditional Access to Sensitive But Unclassified Information Non-Disclosure Agreement"
3. FD Form 258, "Fingerprint Card" (2 copies)
4. Form DHS-11000-9, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
5. Position Designation Determination for Contract Personnel Form
6. Foreign National Relatives or Associates Statement

Required forms will be provided by USCIS at the time of award of the contract. Only complete packages will be accepted by OSI. Specific instructions on submission of packages will be provided upon award of the contract.

Be advised that unless an applicant requiring access to sensitive but unclassified information has resided in the US for three of the past five years, OSI may not be able to complete a satisfactory background investigation. In such cases, USCIS 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 or development of any DHS IT system. USCIS will consider only U.S. Citizens for employment on this contract. USCIS will not approve LPRs for employment on this contract in any position that requires the LPR to access or assist in the development, operation, management or maintenance of DHS IT systems. By signing this contract, the contractor agrees to this restriction. In those instances where other non-IT requirements contained in the contract can be met by using LPRs, those requirements shall be clearly described.

15.3 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 USCIS for acts and omissions of his own employees and for any Subcontractor(s) and their employees to include financial responsibility for all damage or injury to persons or property resulting from the acts or omissions of the contractor's 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.

15.4 Continued Eligibility

If a prospective employee is found to be ineligible for access to USCIS 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 Security Office may require drug screening for probable cause at any time and/ or when the contractor independently identifies, circumstances where probable cause exists.

USCIS 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 USCIS determines to present a risk of compromising sensitive but unclassified 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 USCIS OSI. 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.

OSI must be notified of all terminations/ resignations within five days of occurrence. The Contractor will return any expired USCIS 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.

15.5 Security Management

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the Security Office 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 Security Office 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.

15.6 Computer and Telecommunications Security Requirements

15.6.1 Security Program Background

The DHS has established a department wide IT security program based on the following Executive Orders (EO), public laws, and national policy:

- Public Law 107-296, Homeland Security Act of 2002.
- Federal Information Security Management Act (FISMA) of 2002, November 25, 2002.
- Public Law 104-106, Clinger-Cohen Act of 1996 [formerly, Information Technology Management Reform Act (ITMRA)], February 10, 1996.

- Privacy Act of 1974, As Amended. 5 United States Code (U.S.C.) 552a, Public Law 93-579, Washington, D.C., July 14, 1987.
- Executive Order 12829, *National Industrial Security Program*, January 6, 1993.
- Executive Order 12958, *Classified National Security Information*, as amended.
- Executive Order 12968, *Access to Classified Information*, August 2, 1995.
- Executive Order 13231, *Critical Infrastructure Protection in the Information Age*, October 16, 2001.
- National Industrial Security Program Operating Manual (NISPOM), February 2001.
- DHS *Sensitive Systems Policy Publication 4300A* v2.1, July 26, 2004
- DHS *National Security Systems Policy Publication 4300B* v2.1, July 26, 2004
- Homeland Security Presidential Directive 7, *Critical Infrastructure Identification, Prioritization, and Protection*, December 17, 2003.
- Office of Management and Budget (OMB) Circular A-130, *Management of Federal Information Resources*.
- National Security Directive (NSD) 42, *National Policy for the Security of National Security Telecommunications and Information Systems* (U), July 5, 1990, CONFIDENTIAL.
- 5 Code of Federal Regulations (CFR) §2635, Office of Government Ethics, *Standards of Ethical Conduct for Employees of the Executive Branch*.
- DHS SCG OS-002 (IT), National Security IT Systems Certification & Accreditation, March 2004.
- Department of State 12 Foreign Affairs Manual (FAM) 600, *Information Security Technology*, June 22, 2000.
- Department of State 12 FAM 500, *Information Security*, October 1, 1999.
- Executive Order 12472, *Assignment of National Security and Emergency Preparedness Telecommunications Functions*, dated April 3, 1984.
- Presidential Decision Directive 67, *Enduring Constitutional Government and Continuity of Government Operations*, dated October 21, 1998.
- FEMA Federal Preparedness Circular 65, *Federal Executive Branch Continuity of Operations (COOP)*, dated July 26, 1999.
- FEMA Federal Preparedness Circular 66, *Test, Training and Exercise (TT&E) for Continuity of Operations (COOP)*, dated April 30, 2001.
- FEMA Federal Preparedness Circular 67, *Acquisition of Alternate Facilities for Continuity of Operations*, dated April 30, 2001.
- Title 36 Code of Federal Regulations 1236, Management of Vital Records, revised as of July 1, 2000.
- National Institute of Standards and Technology (NIST) Special Publications for computer security and FISMA compliance.

15.6.2 General

Due to the sensitive nature of USCIS information, the contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume I Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B. This shall include conformance with the DHS Sensitive Systems Handbook, DHS Management Directive 11042 Safeguarding Sensitive but Unclassified (For Official Use Only) Information and other DHS or USCIS guidelines and directives regarding information security requirements. The contractor shall establish a working relationship with the USCIS IT Security Office, headed by the Information Systems Security Program Manager (ISSM).

15.6.3 IT Systems Security

In accordance with DHS Management Directive 4300.1 "Information Technology Systems Security", USCIS Contractors shall ensure that all employees with access to USCIS IT Systems are in compliance with the requirement of this Management Directive. Specifically, all contractor employees with access to USCIS IT Systems meet the requirement for successfully completing the annual "Computer Security Awareness Training (CSAT)." All contractor employees are required to complete the training within 60-days from the date of entry on duty (EOD) and are required to complete the training yearly thereafter.

CSAT can be accessed at the following: <http://otcd.uscis.dhs.gov/EDvantage.Default.asp> or via remote access from a CD which can be obtained by contacting uscisitsecurity@dhs.gov.

15.6.4 IT Security in the Information Technology Lifecycle Management (ITLM) Process

The USCIS OIT ITLM documents all system activities required for the development, operation, and disposition of IT security systems. Required systems analysis, deliverables, and security activities are identified in the ITLM by lifecycle phase. The contractor shall assist the appropriate USCIS ISSO with development and completion of all ITLM activities and deliverables contained in the ITLM. The ITLM is supplemented with information from DHS and USCIS Policies and procedures as well as the National Institute of Standards Special Procedures related to computer security and FISMA compliance. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures. The SSSP shall be based upon the completion of the DHS FIPS 199 workbook to categorize the system of application and completion of the RMS Questionnaire. The SSSP shall be completed as part of the System or Release Definition Process in the ITLM and shall not be waived or tailored.
- *Privacy Impact Assessment (PIA) and System of Records Notification (SORN)*. For each new development activity, each incremental system update, or system recertification, a PIA and SORN shall be evaluated. If the system (or modification) triggers a PIA the

contractor shall support the development of PIA and SORN as required. The Privacy Act of 1974 requires the PIA and shall be part of the ITLM process performed at either System or Release Definition.

- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters. The Contractor shall support annual contingency plan testing and shall provide a Contingency Plan Test Results Report.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA. An ST&E shall be conducted for each Major Application and each General Support System as part of the certification process. The Contractor shall support this process.
- *Risk Assessment (RA)*: This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security. The RA shall be completed after completing the NIST 800-53 evaluation, Contingency Plan Testing, and the ST&E. Identified weakness shall be documented in a Plan of Action and Milestone (POA&M) in the USCIS Trusted Agent FISMA (TAF) tool. Each POA&M entry shall identify the cost of mitigating the weakness and the schedule for mitigating the weakness, as well as a POC for the mitigation efforts.
- *Certification and Accreditation (C&A)*: This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the RA of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation). As appropriate the Contractor shall be granted access to the USCIS TAF and Risk Management System (RMS) tools to support C&A and its annual assessment requirements. Annual assessment activities shall include completion of the NIST 800-26 Self Assessment in TAF, annual review of user accounts, and annual review of the FIPS categorization. C&A status shall be reviewed for each incremental system update and a new full C&A process completed when a major system revision is anticipated.

15.6.5 Security Assurances

DHS Management Directives 4300 requires compliance with standards set forth by NIST, for evaluating computer systems used for processing SBU information. The Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to security requirements are based on the DHS policy, NIST standards and applicable legislation and regulatory requirements. Systems shall offer the following visible security features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own

user ID and password, and each user is authenticated before access is permitted. All system and database administrative users shall have strong authentication, with passwords that shall conform to established DHS standards. All USCIS Identification and Authentication shall be done using the Password Issuance Control System (PICS) or its successor. Under no circumstances will Identification and Authentication be performed by other than the USCIS standard system in use at the time of a systems development.

- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity. Evidence of active review of audit logs shall be provided to the USCIS IT Security Office on a monthly basis, identifying all security findings including failed log in attempts, attempts to access restricted information, and password change activity.
- *Banner Pages* – DHS systems shall provide appropriate security banners at start up identifying the system or application as being a Government asset and subject to government laws and regulations. This requirement does not apply to public facing internet pages, but shall apply to intranet applications.

15.6.6 Data Security

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the DHS Sensitive Systems Handbook and USCIS policies and procedures. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.
- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis

and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.

- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.
- *Data Labeling*. – The contractor shall ensure that documents and media are labeled consistent with the DHS *Sensitive Systems Handbook*.
- **Subpart 4.4—Safeguarding Classified Information within Industry**

4.402 General.

(a) Executive Order 12829, January 6, 1993 (58 FR 3479, January 8, 1993), entitled “National Industrial Security Program” (NISP), establishes a program to safeguard Federal Government classified information that is released to contractors, licensees, and grantees of the United States Government. Executive Order 12829 amends Executive Order 10865, February 20, 1960 (25 FR 1583, February 25, 1960), entitled “Safeguarding Classified Information Within Industry,” as amended by Executive Order 10909, January 17, 1961 (26 FR 508, January 20, 1961).

(b) The National Industrial Security Program Operating Manual (NISPOM) incorporates the requirements of these Executive orders. The Secretary of Defense, in consultation with all affected agencies and with the concurrence of the Secretary of Energy, the Chairman of the Nuclear Regulatory Commission, and the Director of Central Intelligence, is responsible for issuance and maintenance of this Manual. The following DoD publications implement the program:

(1) National Industrial Security Program Operating Manual (NISPOM) (DoD 5220.22-M).

(2) Industrial Security Regulation (ISR) (DoD 5220.22-R).

(c) Procedures for the protection of information relating to foreign classified contracts awarded to U.S. industry, and instructions for the protection of U.S. information relating to classified contracts awarded to foreign firms, are prescribed in Chapter 10 of the NISPOM.

(d) Part 27—Patents, Data, and Copyrights, contains policy and procedures for safeguarding classified information in patent applications and patents.

16.0 Federal Acquisition Regulation (FAR) Clause

The following FAR clause is applicable to the Task Order but has not been specifically addressed previously within this SOW or the contractor’s basic EAGLE contract.

16.1 FAR 52.204-9 Personal Identity Verification of Contractor Personnel (Jan 2006)

(a) The Contractor shall comply with agency personnel identity verification procedures identified in the contract that implement Homeland Security Presidential Directive-12 (HSPD-12), Office of Management and Budget (OMB) guidance M-05-24, and Federal Information Processing Standards Publication (FIPS PUB) Number 201.

(b) The Contractor shall insert this clause in all subcontracts when the subcontractor is required to have physical access to a federally-controlled facility or access to a Federal Information system.

16.2 FAR 52.217-9 Option to Extend the Term of the Contract

(a) The Government may extend the term of this contract by written notice to the Contractor within (30) days within which the Contracting Officer may exercise the option; 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.

17.0 Advertisement, Publicizing Awards, and News Releases.

(a) All press releases or announcements about agency programs, projects, and contract awards need to be cleared by the Program Office and the Contracting Officer. Under no circumstances shall the Contractor, or anyone acting on behalf of the Contractor, refer to the supplies, services, or equipment furnished pursuant to the provisions of this contract in any publicity news release or commercial advertising without first obtaining explicit written consent to do so from the Program Office and the Contracting Officer.

(b) The Contractor agrees not to refer to awards in commercial advertising in such a manner as to state or imply that the product or service provided is endorsed or preferred by the Federal Government or is considered by the Government to be superior to other products or services.

