Company Name:
Science Applications International Corporation (SAIC)

Contract Number:
HSHQDC-06-D-00026 (HSHQDC06D00026)

Order Number:
HSCETC-09-J-00018 (HSCETC09J00018)

Requisition/Reference Number:
192109CIOSDD1TH20

Period of Performance:
9/30/2009 through 12/31/2013

Latest Modification Processed:
N/A

Services Provided:
Provides the Enterprise Acquisition Gateway for Leading Edge Solutions (EAGLE) Functional Category 4 for Services Oriented Architecture (SOA), Web Services, and Law Enforcement Information Sharing Service (LEISS).

ORDER FOR SUPPLIES OR SERVICES

PAGE 1 OF PAGES 74

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

1. DATE OF ORDER: 09/29/2009	2. CONTRACT NO. (If any): HSHQDC-06-D-00026
3. ORDER NO.: HSCETC-09-J-00018	4. REQUISITION/REFERENCE NO.: 192109CIOSDD1TH20

5. ISSUING OFFICE (Address correspondence to):
ICE/Info Tech Svs/IT Services
Immigration and Customs Enforcement
Office of Acquisition Management
801 I Street NW, Suite 930
Washington DC 20536

6. SHIP TO:
a. NAME OF CONSIGNEE: ICE Chief Information Officer
b. STREET ADDRESS: Immigration and Customs Enforcement
801 I Street, NW
Suite 700
c. CITY: Washington | d. STATE: DC | e. ZIP CODE: 20536

7. TO:
a. NAME OF CONTRACTOR: SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
b. COMPANY NAME:
c. STREET ADDRESS: 10260 CAMPUS POINT DRIVE
MAIL STOP G2
d. CITY: SAN DIEGO | e. STATE: CA | f. ZIP CODE: 921211522

f. SHIP VIA:

8. TYPE OF ORDER
☐ a. PURCHASE
REFERENCE YOUR:
Please furnish the following on the terms and conditions specified on both sides of this order and on the attached sheet, if any, including delivery as indicated.
☒ b. DELIVERY
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))
☐ a. SMALL ☒ b. OTHER THAN SMALL ☐ c. DISADVANTAGED ☐ g. SERVICE-DISABLED VETERAN-OWNED
☐ d. WOMEN-OWNED ☐ e. HUBZone ☐ f. EMERGING SMALL BUSINESS

12. F.O.B. POINT: Destination

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

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: [redacted] The Government accepts Science Applications Internationals Corporations (SAIC) proposal for Web Services dated September 29, 2009. This Task Order will be a hybrid contract of Cost Plus Fixed Fee (CPFF), Firm Fixed Continued ...					

18. SHIPPING POINT	19. GROSS SHIPPING WEIGHT	20. INVOICE NO.	17(h) TOTAL (Cont. pages): [redacted]

21. MAIL INVOICE TO:

SEE BILLING INSTRUCTIONS ON REVERSE

a. NAME: DHS, ICE — $1,000,000.00

b. STREET ADDRESS (or P.O. Box): Burlington Finance Center
P.O. Box 1620
Attn: ICE-OCIO-SDD

17(i) GRAND TOTAL: [redacted] — $1,000,000.00

c. CITY: Williston | d. STATE: VT | e. ZIP CODE: 05495-1620

22. UNITED STATES OF AMERICA BY (Signature): [redacted]

23. NAME (Typed): Maxine D. Edwards
TITLE: CONTRACTING/ORDERING OFFICER

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/30/2009	HSHQDC-06-D-00026	HSCETC-09-J-00018

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	Price (FFP) and Cost Reimbursable (CR) awarded under EAGLE. Points of Contact: Contracting Officer: Maxine Edwards 801 I Street N.W., Suite 900 Washington, DC 20536 (202) 732- b6 b6 Contract Specialist: Kimberlee Brown 801 I Street N.W., Suite 900 Washington, DC 20536 (202) 732- b6 b6 Contracting Officer Technical Representative: Scott A. Johnson 801 I Street, N.W. Washington, DC 20536 (202) 306- b6 (305) 675-8373 Fax b6 Period of Performance: 09/30/2009 to 12/31/2013					
0001	Base Period Period of Performance:9/30/2009 thru 12/31/2009 Accounting Info: Funded: $0.00	1	LO		0.00	
0001A	Transition In (CPFF) Product/Service Code: D302 Product/Service Description: ADP SYSTEMS DEVELOPMENT SERVICES Continued ...	1	LO		0.00	

TOTAL CARRIED FORWARD TO 1ST.PAGE (ITEM 17(H)) $0.00

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/30/2009	HSHQDC-06-D-00026	HSCETC-09-J-00018

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
0001B	Development Labor (CPFF) Fully Funded Obligation Amount$ b4 Incrementally Funded Amount: $ b4 Accounting Info: b2High Funded: $ b4	1	LO	b4		
0001C	Fixed Fee (FF) for CLIN 0001B Accounting Info: b2High Funded: $ b4	1	LO	b4		
0001D	Operation and Maintenance (FFP) (O&M $ b4 / month) Accounting Info: b2High Funded: $ b4	1	LO	b4		
0001E	Hardware and Software Equipment (CR)	1	LO		0.00	
0001F	Other Direct Cost (ODCs)- Travel (CR) Not to exceed $ b4 . Accounting Info: b2High Funded: $ b4	1	LO	b4		
0001G	Optional Task (s)	1	LO		0.00	
1001	Option Year One Period of Performance: 01/01/2010 thru 12/31/2010	1	LO		0.00	
1001A	Development Labor (CPFF) (Option Line Item) Continued ...	1	LO	b4	0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $1,000,000.00

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/30/2009	HSHQDC-06-D-00026	HSCETC-09-J-00018

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
1001B	Fixed Fee (FF) for CLIN 1001A (Option Line Item)	1	LO	b4	0.00	
1001C	Operation and Maintenance (FFP) (O&M $ b4 /month) (Option Line Item)	1	LO	b4	0.00	
1001D	Hardware and Software(CR) (Option Line Item)	1	LO		0.00	
1001E	Other Direct Cost (ODCs) - Travel (CR) Not to exceed $ b4 . (Option Line Item)	1	LO	b4	0.00	
1001F	Optional Task (s) (Option Line Item)	1	LO		0.00	
2001	Option Year Two Period of Performance: 01/01/2011 thru 12/31/2011	1	LO		0.00	
2001A	Development Labor (CPFF) (Option Line Item)	1	LO	b4	0.00	
2001B	Fixed Fee (FF) for CLIN 2001A (Option Line Item)	1	LO	b4	0.00	
2001C	Operation and Maintenance (FFP) (O&M $ b4 month (Option Line Item)	1	LO	b4	0.00	
2001D	Hardware and Software Equipment (CR) (Option Line Item)	1	LO		0.00	
2001E	Other Direct Cost (ODCs) - Travel (CR) Not to exceed $ b4 . (Option Line Item)	1	LO	b4	0.00	
2001F	Optional Task(s) (Option Line Item)	1	LO		0.00	
3001	Option Year Three Period Of Performance: 01/01/2012 thru 12/31/2012	1	LO		0.00	

Continued ...

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $0.00

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/30/2009	HSHQDC-06-D-00026	HSCETC-09-J-00018

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
3001A	Development Labor (CPFF) (Option Line Item)	1	LO	b4	0.00	
3001B	Fixed Fee (FF) for CLIN 3001A (Option Line Item)	1	LO	b4	0.00	
3001C	Operation and Maintenance (FFP) (O&M $ b4 /month (Option Line Item)	1	LO	b4	0.00	
3001D	Hardware and Software Equipment (CR) (Option Line Item)	1	LO		0.00	
3001E	Other Direct Cost (ODCs)- Travel (CR) Not to exceed $ b4 . (Option Line Item)	1	LO	b4	0.00	
3001F	Optional Task(s) (Option Line Item)	1	LO		0.00	
4001	Option Year Four Period of Performance:01/01/2013 thru 12/31/2013	1	LO		0.00	
4001A	Development Labor (CPFF) (Option Line Item)	1	LO	b4	0.00	
4001B	Fixed Fee (FF) for CLIN 4001A (Option Line Item)	1	LO	b4	0.00	
4001C	Operation and Maintenance (FFP) (O&M $ b4 /month (Option Line Item)	1	LO	b4	0.00	
4001D	Hardward and Software Equipment (CR) (Option Line Item)	1	LO		0.00	
4001E	Other Direct Costs (ODCs)- Travel (CR) Not to execced $ b4 . (Option Line Item)	1	LO	b4	0.00	
4001F	Transition Out (CPFF) (Option Line Item)	1	LO	b4	0.00	
4001H	Optional Task(s) (Option Line Item) Continued ...	1	LO		0.00	

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $0.00

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

DATE OF ORDER	CONTRACT NO.	ORDER NO.
09/30/2009	HSHQDC-06-D-00026	HSCETC-09-J-00018

ITEM NO. (a)	SUPPLIES/SERVICES (b)	QUANTITY ORDERED (c)	UNIT (d)	UNIT PRICE (e)	AMOUNT (f)	QUANTITY ACCEPTED (g)
	The total amount of award: $41,727,032.75. The obligation for this award is shown in box 17(i).					

TOTAL CARRIED FORWARD TO 1ST PAGE (ITEM 17(H)) $0.00

Section B: Supplies/Services Price/Cost Schedule

B.1 Price/Cost Schedule

The Contractors labor categories, and labor hours for all contract years are in Attachment 4.

B.2 Items To Be Acquired

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

B.3 Ordering Activity

The Department of Homeland Security (DHS), Immigrations and Customs Enforcement is the sole authority to request services under this task order.

B.4 Contract Ceiling

The ceiling for this task order is $41,727,032.75 plus an estimated $6,752,500.11 for optional task for a total contract ceiling of $ 48,479,532.86.

B.5 Type Of Contract

This task order is hybrid of cost plus fixed fee, firm fixed price with a cost reimbursable CLIN for Hardware, Software and Travel which will be issued off of the DHS EAGLE contract under Functional Category 4. All terms and conditions of the DHS EAGLE contract apply to this task order.

B.6 North American Classification System (NAICS)/ Product Service Codes (PSC)

NAICS Code: 541512, Information Management Computer Systems Integration Design Services

PSC Code: D302, ADP System Development

B.7 Definition

This solicitation uses the term "contract" to include task order.

Section C: Statement of Work

U.S. Department of Homeland Security
Immigration and Customs Enforcement

Office of the Chief Information Officer

Systems Development Division

Services Oriented Architecture (SOA), Web Services, and Law Enforcement Information Sharing Service (LEISS)

C.1 PROJECT TITLE

Services Oriented Architecture (SOA), Web Services, Law Enforcement Information Sharing Service (LEISS)

C.2 BACKGROUND

This task will support the Department of Homeland Security (DHS), Immigration and Customs Enforcement (ICE), System Development Division (SDD), Investigative Systems Branch (ISB), Detention and Removal Office (DRO). The ISB is responsible for providing information technology support services in the development, implementation, and maintenance of agency software applications. The branch's specific responsibility is for the maintenance and enhancement of applications that support law enforcement activities. The work described below is presently being performed under the Information Technology Engineering Support Services (ITESS) Task Order COW-5-D-0056, Task R.

In an effort to ensure the successful execution of the ICE LEISS initiative, the agency continues to expand its development, maintenance, and support of web services. These web services shall provide mission-critical production dependencies to systems inside and outside of ICE by allowing multiple applications from several sources to communicate with each other using open protocols. In addition, this task will support ICE coordination efforts with program managers of other sharing systems to ensure a high level of quality for ICE data offerings.

Web services are methodologies for providing distributed software services across a network. These software systems are designed to support interoperable machine-to-machine interaction. The basis for web services is Extensible Markup Language (XML), which provides a language that can be used between different platforms and programming languages to express complex messages and functions.

Web services platform elements include:

- Simple Object Access Protocol (SOAP) - a protocol specification for exchanging structured information in the implementation of web services in computer networks
- Universal Description, Discovery and Integration (UDDI) - a platform-independent, XML-based registry for businesses worldwide to list themselves on the Internet
- Web Services Description Language (WSDL) - an XML-based language that provides a model for describing Web services

Web services provide mission-critical production dependencies to systems inside and outside of ICE and operate to ensure the following:

- Support for mission-critical systems without interruption
- Address of potential functional enhancement and enterprise refactoring
- Promotion and furtherance of the Service Oriented Architecture (SOA) initiative through technical leadership, SOA consultation, and maturation

Web services have been developed to act as the autonomous endpoints, and when combined, will serve as a registry for services aggregation in the SOA initiative. As the implementation of services matures, the aggregation may be realized as coupled services. Enterprise Service Bus (ESB) and/or Business Process Execution Language (BPEL) can be realized as a result of technical integration efforts that include the use of DataPower, WebSphere, and other IT capital that form the infrastructure for SOA at ICE.

The LEISS Web Service was developed to facilitate the sharing of information from ICEPIC with Federal, State, and local law enforcement agencies via implementation of web services. The LEISS Web Service was originally implemented using the ICE architecture, LEXS 2.0 and the DataPower appliance. The service offerings have recently expanded to include the implementation of LEXS 3.1 in addition to LEXS 2.0. This web service allows users to submit queries on names, dates, addresses, and numbers, and enables users to view responses that contain structured and unstructured data about cases. Additional information such as narrative data on case subjects and attachments can be shared using the latest version of LEXS, which includes fingerprints and photos. The LEISS Web Service will return data held in the ICEPIC database that has been selected, filtered, and reviewed in accordance with information sharing agreements reached between any cooperating Federal, State and local agencies and with state and federal laws.

C.3 SCOPE OF WORK

This Statement of Work (SOW) document outlines the current high-level functional and technical requirements for the Office of the Chief Information Officer (OCIO), DHS, ICE, ISB and DRO for the development, configuration, customization, installation, testing, training, documentation, and support of web services to ensure integration of the ICE SOA initiative for the ISB. This includes the support of web services developed specifically for LEISS and other requirements detailed in the specific tasks. These web services support mission-critical systems while supporting ICE and DHS initiatives in information sharing and modernization. Task (4.1 – 4.5) are required to be performed the base period. Tasks 4.6 – 4.11 are required to be performed in the option years.

The Contractor shall provide the project management and development personnel assistance to align ICE technology with ICE business requirements and to manage initiatives in SDD as directed by SDD personnel. The Contractor shall support and develop web services while integrating the technical architecture standards, providing systems assurance support, collecting user feedback from ICE personnel and external

users of ICE data, conducting development and functional testing, and aligning with Enterprise Architecture (EA) planning efforts throughout ICE.

The Contractor shall ensure that the following processes are integrated:

- ICE Systems Lifecycle Management (SLM)
- Information Systems Security
- Certification and Accreditation (C&A)
- Capital Planning and Investment Control (CPIC)

The Contractor shall support the integration of web services, including the LEISS Web Service, to ensure the successful execution of the SOA within the U.S. DHS environment. The LEISS Web Service is a specific web service that was developed to facilitate the sharing of information from the ICE Pattern Analysis and Collection System (ICEPIC) databases with Federal, State, and local law enforcement agencies. The LEISS Web Service was established as an SOA that follows the National Information Exchange Model (NIEM) and the LEISP Exchange Specifications (LEXS) to interface with the ICEPIC data warehouse and multiple data systems used by other law enforcement agencies. This web service initiative is one of several tasks to be accomplished in order to achieve the initial goal of sharing information between ICE and Federal, State, and local law enforcement agencies.

ICE is consolidating all its development, testing, production, and disaster recovery environments to the two DHS Enterprise Data Centers. Any development work done under this contract will only ever be implemented at a DHS Enterprise Data Center. Implementation at DHS
Enterprise Data Centers includes having production, development, testing and Disaster Recovery environments at DHS Enterprise Data Centers. Development work includes enhancements, adding functionality, or providing increased capability. ICE plans to migrate LEISS to DHS Enterprise Data Centers in 2011.

Support of the systems hosted outside of DHS Enterprise Data Centers is limited to operations and maintenance. Neither development, nor enhancements, nor adding functionality, nor providing improved capability to systems hosted outside of DHS Enterprise Data Centers is
allowed under this contract.

The Contractor shall furnish all personnel, technical expertise, equipment, materials, transportation as well as other items or services necessary to perform the work described in this SOW (except those specified as Government-Furnished Equipment (GFE) or information).

C.4 SPECIFIC TASKS

C.4.1 Operations and Maintenance

The Contractor shall manage and maintain web services for LEISS, Student and Exchange Visitor Information System (SEVIS), Enterprise Alien Removals Module (EARM) and any new developments under this SOW. The Contractor shall also identify and correct software, performance, and implementation failures. This web service maintenance includes performing emergency repairs when immediate corrections are necessary, continue user service and, corrective work which includes performing System Change Requests (SCRs) that reflect the requirements/specifications, and updating and maintaining the required SLM documentation as necessary.

Software changes to applications are based upon the submission and Government approval of an SCR. The Contractor shall be responsible for carrying out all application maintenance requirements projects including opening SCRs and entering the data in the ICE approved management tracking tool. Prior to commencing a system modification, the Contractor and the OCIO Program Manager shall agree on the degree of the modification as minor, moderate, or major. (See table below for classification).

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

Emergency maintenance shall be performed at the direction of the Government. The respective OCIO Program Manager must approve all SCRs in writing.

The following requirements apply to each of the tasks:

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

The Contractor shall fully maintain the web services and software developed under this SOW. Tasks include, but are not limited to:

- Perform maintenance tasks to meet changes in requirements of the users or user environment, enhance the system to provide additional or changed functionality, and adapt the system to changes in business processes, or extend software to new users.

- Provide coordination with ICE Headquarters and field personnel, including prepare information to be disseminated to customers, including brochures and informational sheets.
- Meet with the ICE Headquarters Program and Policy personnel regarding the technical issues on a weekly or as needed basis.
- Coordinate with ICE Help Desk and ICE Program Manager to provide technical support to ICE Headquarters, Monday to Friday, 6am to 6pm EST/EDT. This includes, but may not be limited to:
    - Provide Tier 2 and 3 Help Desk Support from 8:00 AM to 8:00 PM EST Monday through Friday (except for federal holidays) over the telephone. ICE will provide Tier 1 services using the ICE Remedy System. The Contractor shall provide Tier 2 and Tier 3 services using the remedy system as well. Access to the ICE Remedy System will be provided to the Contractor. Tier 1 support consists of receiving initial requests for service, providing telephone assistance in resolving the reported problem, tracking the request from receipt of call to completion of service or escalating calls to the next level as required, and issuing customer surveys.
- Provide Tier 2 and 3 Help Desk Support. This support includes:
    - Specific questions/problems that Tier 1 (which is handled by ICE Help Desk) is unable to resolve.
    - Issues that must be coordinated with ICE Government IT personnel.
    - Specific requests that must be coordinated with database administrators to perform data fixes to records.
    - Generate statistical, workload, and trend analysis reports in addition to reports that ICE Application Hosting Services (AHS) can provide.
    - Develop updated SOPs, scripts, and procedures for Tier 2 and 3 Help Desk staff to use when new information, releases, or changes regarding ICEPIC have been distributed and/or implemented.
- Provide comprehensive administrative support for the web services production environment, which includes ensuring that all components are operational 24/7.
- Provide support for collection and processing of metrics.

C.4.2 Web Services Support

The Contractor shall provide the project management and development personnel with SOA and the development of web service experience along with knowledge of the ICE SOA architecture.

The Contractor shall establish and maintain a service-based infrastructure for SEVIS and EARM. This will include, but is not limited to:

- Supporting services in WebSphere, or migrating as directed to other development environments.
- Providing continued maintenance and updates to the services.
- Creating or updating SLM documentation of the hardware and software architecture, configuration, and interfaces.
- Providing support and maintenance of the services including:
  - Address of new functionality
  - Orchestration of services in distributed network transactions
  - Integration of IT infrastructure components (as necessary)

The Contractor shall support the building of new web services as deemed by the customer in support of the SOA initiative. The new web services will include, but are not limited to:

- Adhere to the SLM Standards defined in section 5.1.
- Conducting development, functional, integration and system testing, installation, iinplementation, and support of web services.
- These services will support ICE in the following areas, but are not limit to:
  - Information sharing
  - Booking services
  - Person-centric queries
  - Insert and update services

C.4.3 LEISS

The Contractor shall provide the project management and development personnel with knowledge for information sharing, LEXS, NIEM, SOA and the web service development experience along with knowledge of the ICE SOA architecture.

The Contractor shall continue to support development efforts by:

- Complying with current versions of LEXS standards
- Developing and supporting message audit logs
- Hardening access points for XML validation
- Building a robust aggregation service to include SLM documentation of the hardware and software architecture, configuration, and interfaces
- Supporting necessary hardware used by the service as needed

- Provide new functionality to support the needs of the business or changes in business functionality

In an effort to support the LEISS Web Service task, LEISS shall:

- Share DHS person-centric case information with law enforcement agencies
- Allow agencies to access certain DHS information from the data stored in the ICEPIC database
- Use the Global Justice XML Data Model (GJXDM) and NIEM to comply with the LEISS Exchange Specifications (LEXS) data exchange information
- Transform LEXS messages to XML based Universal Message Format (UMF) to query data base
- Provide rapid response to law enforcement users
- Adhere to DHS information sharing governance
- Provide the development of enhancements in support of changes to the ICEPIC application.

In support of the LEISS project the Contractor shall:

- Support and manage current connections to federal, state, and local law enforcement agencies
- Work with OCIO,OI, and DRO to expand the consumer base of law enforcement agencies
- Ensure information sharing technologies and operational policies that are established by ICE and law enforcement community
- Provide additional web services or application software in support of the DHS and ICE information sharing initiative as needed

C.4.4 Improvements to LEISS Operational Performance

- Coordinate regional feedback from both internal and external users to the ICE user community to improve the impact of information sharing
- Visit key sites of external users from the information sharing communications to assess ICE DHS data rendered in their systems to offer and improve the quality of the data and its effectiveness for its internal user.

C4.5 Transition Support

C.4.5.1 Transition Plan (In)

The Contractor shall be responsible for the transition of all technical activities identified in this Task Order (TO). The Contractor shall submit a final detailed Transition Management Plan (TMP) 5 business days after the kickoff meeting, which reflects the completed transition activities 60 calendar days after the kickoff meeting. The technical activities included as part of the technical transition plan are:

- Inventory and orderly transfer of all Government Furnished Equipment/Property (GFE/GFP), software, and licenses
- Transfer of documentation currently in process
- Transfer of all software coding in process
- Coordination of the body of work with the Incumbent Contractor and receipt of tasking, ad hoc queries, reports, procedures, etc.

The Contractor's TMP shall be approved by Program Manager/COTR and shall contain a milestone schedule of events and system turnovers. The TMP shall transition systems with no disruption in operational services.

C.4.5.2 Transition Plan (Out)

The Contractor shall be responsible for the transition of all technical activities identified in this task. The Contractor shall provide a TMP 120 calendar days prior to the completion of the period of performance of this contract. The Contractor's TMP shall be approved by Program Manager/COTR and shall contain a milestone schedule of events and system turnovers. The Contractor shall complete the transition period within 60 calendar days before the completion of the period of performance of this contract. The technical activities, which shall be included as part of the technical transition plan consists of the following:

- Inventory and orderly transfer of all Government Furnished Equipment/Property (GFE/GFP), software and licenses
- Transfer of documentation currently in process
- Transfer of all software coding in process
- Coordinate transition with DHS/ICE IT personnel
- Coordinating the body of work with the current Contractor and turnover of tasking, ad hoc queries, reports, procedures, etc.

The Contractor shall fully support the transition of Systems Development requirements to the successor. The TMP shall transition systems with no disruption in operational services. Responsibilities include supporting all of the activities listed above by making available personnel and documentation required to facilitate a successful transition.

C.4.6 Support growth of capabilities of the Alien Criminal Response Information Management System (ACRIMe) to Law Enforcement Service Center (LESC) using LEISS

Integrate LEISS and ICEPIC capabilities with ACRIMe in support of the LESC to provide automated and rapid response to field requests for confirmation about suspects or detained personnel. Under this task order the Contractor shall provide System Engineering and Software Development support to expand current LEIS Services and develop applications that route queries from ICE agents and Local Law Enforcement officials in the field to the LESC, conduct a search into DHS data sources, and return a response to the requestor of the status of the individual under scrutiny. This process will initially augment, not replace, the current LESC process that includes an ICE Agent as the releasing authority for information. The Contractor shall provide the program management and technical personnel in support of the full lifecycle requirement analysis, design, development, integration, and implementation of integration of LEISS into ACRIMe.

The Contractor shall provide the following specific services in support of full lifecycle development of this integration, which shall include, but are not limited to:

- Provide requirements analysis, design, development, all levels of testing, and implementation support for the integration of LEISS with ACRIMe system.
- Integrate the LEIS Service with the ACRIMe system.
- Adhere to the System Lifecycle Management Standards defined in section 5.1.

This task will be optional in the base period of the contract, but will be required in the option years.

C.4.7 Conduct Capability Gap Analysis Study of Systems Integration and Information Sharing of Field Operations

Conduct a Gap Analysis Study with the goal to provide a concept description for a baseline assessment to chart all Information Sharing capabilities, supporting technologies, gaps in coverage, and plans, processes, techniques and procedures throughout the Department and between interagency and international partners. This assessment will provide a way-ahead for effective systems integration,

capability improvements and will provide specific recommendations for achieving an integrated Information Sharing end state.

An integrated Information Sharing IT infrastructure supporting the right interagency processes, procedures, and protocols, would allow for the integration and fusion of vast amounts of data from multiple sources. Fusion and analysis of this data, in conjunction with national or international law enforcement and intelligence data can provide a better multi-domain awareness and knowledge management framework that supports Local, State, and National Homeland Security goals and objectives. By incorporating proven approaches and techniques to establish and maintain accurate domain and situational awareness, an integrated information sharing strategy can better support security and defense critical missions, and would also provide the added benefit of enhancing regional commerce and trade.

An integrated Information Strategy infrastructure could better support the following functions:

- Gather multi-domain information from the various DoD, interagency, and law enforcement fusion and operation centers, as determined by the Department
- Integrate and fuse data from disparate sources and entities
- Provide intelligence analysis with experienced specific domain experts
- Share and Disseminate critical and relevant information on a time sensitive basis
- Monitor and track vessels, aircraft, vehicles, people and goods
- Use predictive and probabilistic tools to identify potential threats
- Support simulations or scenarios of potential events for training purposes
- Interact with local, state, national and international law enforcement and Homeland Security organizations

An effective Information Sharing infrastructure and processes represents:

- A critical tool to keep our nation safe
- A fundamental and integral part of the Homeland Security Plan, supporting national security objectives
- A highly effective capability that supports US and partner nation agencies preparing crisis response and to identify, protect, simulate and respond to various threats

By mapping legacy systems, IT infrastructure, as well as the various standards, methods, techniques and procedures for information processing and

dissemination, DHS/ICE can develop a workable blue print that would effectively support the various ongoing interagency integration efforts.

A baseline assessment would:

- Assess legacy IT systems/applications and systems under development throughout the various organizations and intelligence centers
- Assess capability requirements and map legacy standards, methods, techniques and procedures
- Recommend cost-benefit solutions to integrate information systems, and processes

This task will outsource an experienced senior Contractor team to conduct this assessment. Notionally, the effort would consist of team senior analysts (with experience in IT systems, intelligence, interagency, knowledge management and law enforcement coordination).

This task will be optional in the base period of the contract, but will be required in the option years.

C.4.8 Metrics Development and Reporting Team

Gather key metrics for LEISS usage (internal and external to DHS), ICEPIC usage, data ingestion, and systems (Hardware and services) monitoring. Develop reports that indicate Performance Measures of Effectiveness, Risks, Vulnerabilities, Systems Up/Down Times (performance), Usage, etc. The Contractor shall provide the following specific services in support of the requirement analysis, metrics analysis, design, development, integration, and implementation of metric reporting for LEISS and ICEPIC usage, which will include, but are not limited to:

- Provide requirements analysis, metrics analysis, design, development, all levels of testing, and implementation support for the metric reporting for LEISS and ICEPIC usage.
- Provide a comprehensive description of the proposed technical approach prior to commencing this task.
- Ensure integration into the LEISS and ICEPIC system environment.
- Adhere to the System Lifecycle Management Standards defined in section 5.1.

This task will be optional in the base period of the contract, but will be required in the option years.

C.4.9 Expansion of Services for International Sharing Communities

Develop the infrastructure and policies for establishing a Services Oriented Architecture (SOA) to allow Information Sharing on an International level. Working with the Office of International Affairs (OIA), OI, DHS Law Enforcement Information Sharing Initiative, Office of Intelligence and Analysis, DRO, and the OCIO, this task will include development of information sharing requirements, identification of information sources, recommendations for acquisition of information systems, implementation and development of the hardware and software infrastructures, and operational management of the infrastructure. The Contractor shall provide the following specific services in support of developing the infrastructure and policies for Information Sharing on an International level, which will include, but are not limited to:

- Conduct a formal Functional Requirements Study, requirement gathering, and requirement analysis to develop the Functional Requirements Document (FRD).
- Conduct interviews with user groups to ensure all requirements are captured for all levels and types of users.
- Ensure the FRD includes a solution that consolidates, standardizes, and centralizes the agency law enforcement information and applications relevant to the ISB.
- Conduct research, requirements analysis, and requirements gathering techniques to create a detailed System Requirements Document (SRD) while satisfying all conditions required by the ICE OCIO Architecture Division.
- Coordinate with the ISB Program Office to analyze the Mission Support businesses, data, and reports for inclusion in the final solution.
- Develop a strategy framework and policy for Information Sharing on an International level.
- Development of Standard Operation Procedures (SOP) for operational management of the infrastructure.
- Adhere to the System Lifecycle Management Standards defined in section 5.1.

This task will be optional in the base period of the contract, but will be required in the option years.

C.4.10 Direct Support to Law Enforcement Sharing Initiative

Provide OCIO direct support to the Law Enforcement Sharing Initiative in the (OI) and DRO. This support will include development of technical documentation to support Service Level Agreements and Inter-Service Agreements, as well as articulate documented requirements that originate from the Executive Information Unit (EIU)/OI.

This task will be optional in the base period of the contract, but will be required in the option years.

C.4.11 Development of services to manage access via role-based methodology

The Contractor shall create and implement a policy and procedures for the user to access specific data sets via the LEISS. This task requires the recommendation of policy and procedures for controlling access based on user role, and interface to the DHS and external sharing partners' tools which facilitate exchange and access to data.

This task will be optional in the base period of the contract, but will be required in the option years.

C.5 GENERAL REQUIREMENTS

C.5.1 System Lifecycle Management Standards

The Contractor shall provide the following specific services in support of full systems lifecycle development process for each development task defined in this Statement of Work, which will include, but are not limited to:

- Providing requirements analysis, design, development, all levels of testing, and implementation of the system based on the FRD.
- Conducting research, requirements analysis, and requirements gathering techniques to create a detailed System Requirements Document (SRD) while satisfying all conditions required by the ICE OCIO Architecture Division.
- Providing design, development, all levels of testing, and implementation support according to the SRD, as well as any open SCRs approved by the OCIO Project Manager and the CCB. Prior to commencing a system modification or SCR, the Contractor and the OCIO Project Manager shall agree on the level of effort of the modification.
- Follow detailed guidance contained within the SRD and the expected timing for delivery of functionality.
- Providing a comprehensive description of the proposed technical approach prior to commencing this task.
- Ensuring that the application is subjected to all levels of testing, ranging from unit to UAT.
- Ensuring seamless integration into the ICE technical architecture.

- Coordinating with ICE technical personnel to establish the dynamic links to the external system identified as supporting interfaces.
- Ensuring that the solution developed will scale to an enterprise application.
- Providing all application interface design and development while adhering to the ICE technical architecture standards.
- Creating or updating all SLM documentation of the hardware and software architecture, configuration, and interfaces.
- Ensuring scalability that allows for future incorporation of additional modules or functions.
- Ensuring that the development of the systems identified in the Statement of Work, all future enhancements, and SCRs satisfy all conditions required by the ICE OCIO Architecture Division.
- Adhering to the ICE technical architecture standards.
- Developing system user guides, help files, and context-sensitive help information that will be incorporated into the application.
- Designing the development and test environments in compliance with ICE OCIO\AHS such that it can be hosted at the DHS data center.
- Meeting FISMA security requirements to protect against the loss of sensitive information.

C.5.2 Performance Standards

The Contractor shall comply with all technology standards and architecture policies, processes, and procedures defined in the ICE Office of the Chief Information Officer (OCIO) Architecture Division publications.

The Contractor shall be expected to conform to ICE recommended architecture and to comply with ICE technical standards. Use of Commercial Off-The-Shelf (COTS) products for components that match very closely to Government requirements are acceptable, however the Contractor is responsible for confirming that all COTS products proposed may be deployed in the ICE standard environment on ICE standard infrastructure as articulated in the supporting materials. Contractors are responsible for listing all COTS dependencies which conflict with the ICE standard environment, as well as stating how they intend to mitigate such conflicts. Furthermore, the Contractor is responsible for costs incurred to resolve undisclosed dependencies which conflict with ICE standards.

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

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

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

Note: The ICE SLM process closely follows the DHS System Enterprise Lifecycle (SELC) process and the Contractor shall only have to adhere to the former.

C.5.3 Configuration Management

The Contractor shall be responsible for configuration management for all design and development tasks under the guidelines set forth by the ICE OCIO Architecture Division. ICE-approved configuration management tools will be provided by the Government for use by the program team. The Government requires that all formal product baseline submissions (as defined by the SLM Process) be checked into the ICE-approved configuration management repository. Use of any other configuration management tool in conjunction with this requirement must meet Government configuration management functional, security, and audit requirements and be set forth in the Contractor 's formally submitted SLM Configuration Management Plan. The Contractor shall conduct project-level configuration management for all design and development work for the applications, database, or configurable component; execute all approved requests for changes to establish new baselines via the approved System Change Request (SCR) process, including the chartering and conducting Change Control Board (CCB) meetings; assign proper identification of all configuration items in accordance with agreed on conventions. This includes the proper labeling of all software releases, regardless of content, and submitting an electronic version of all deliverables to the Electronic Library Management System (ELMS) library.

C.5.4 Compliance with Architecture

In support of DHS architecture standards and guidelines, ICE OCIO has developed a standard architectural framework and has deployed shared infrastructure to support the implementation and integration of the proposed

solution. The architecture has been defined to support a very broad range of solutions needed to meet a variety of functional and non-functional requirements. The Contractor is expected to propose a solution within the boundaries of the ICE standard architecture; however the Contractor shall request use of solution components and technologies not currently specified in the ICE standard architecture through the deviation procedure described in Standards and Processes.

The Government will provide all Offerors with detailed information regarding architectural guidelines. The Contractor shall be responsible for ensuring the proposed solution can be implemented within the ICE standard architecture at the cost proposed and on the schedule proposed in the Contractor's final proposal. The Contractor shall request clarifications to aspects of the architecture not fully understood by the bidder during the RFI/RFP process. All prospective Offerors shall be provided with requested clarifications and question responses.

Should the Contractor subsequently determine that it is unable to produce the proposed solution in the ICE architecture (non-transparent changes made by the Government to the architecture withstanding) without impacting cost or schedule, the Government retains the option of requiring the Contractor to modify the contract to add an additional third party service or product provider (as specified by the Government) in order to fill potential offering gaps.

Note: The ICE OCIO is moving increasingly towards a modular, flexible, Services Oriented Architecture (SOA) and away from information and functionality silos. Proposed solutions are fully expected to be compatible with ICE architectural *philosophy* as well as specific product and technology standards.

C.5.4.1 Portal and Presentation Services

The Contractor shall implement a central access point or interface that creates a tailored user experience suitable for different user roles involved in the business process. Portal and Presentation tier capability must be available through ICE standard Internet Explorer browser interfaces, with flexibility to deploy some functionality to portable devices as well as disconnected clients where indicated by requirements.

C.5.4.2 Application Services

Web Services will utilize an applications services tier based on ICE's shared Application Hosting Platform (AHP). Application and service components will be developed and deployed in this layer of the architecture. Business logic specific for implementation of a well defined, loosely coupled component can be developed at this level.

C.5.4.3 Enterprise Service Bus (ESB)

ICE utilizes multi-tier service bus architecture to secure services, perform commodity service functions, execute business process workflows, manage business process orchestration, and perform data/process aggregation. Many business processes will be defined during requirements which are suitable for actualization on ICE's extended service bus platform. Business processes may be both event driven as well as invocation driven. The Contractor shall be expected to complete integration of processes, develop components, and bind processes to realized components. The Contractor shall **not** be expected to design or implement an ESB platform for ICE or ICE systems.

Workflow and automation of manual tasks will be primarily performed in this tier of the architecture. The Contractor's design and implementation should provide substantial flexibility for evolving and replacing components, adjusting business processes dynamically, as well as selectively replacing manual tasks with automated tasks as capabilities evolve.

C.5.4.4 Authorization and Access Control

The Contractor shall be expected to fully utilize ICE's single sign on environment for user authentication as well as role based authorization that can be suitably defined within the enterprise directory. Authorization rules not suitable for the ICE single sign on environment may be handled within proposed solution components.

C.5.4.5 Logging and Auditing

The Contractor shall leverage enterprise level logging and auditing infrastructure for the storage, management, archiving, and access of logs and audit records generated by the application.

C.5.4.6 Data Tier

The Contractor shall leverage ICE's highly available Oracle Enterprise hosting environment for all data storage needs, excepting situations where specific COTS components used to implement necessary functions require another product for data tier. Information models for custom components will be produced by the Contractor and must be consistent with ICE Enterprise Data Modeling standards as well as business object definitions specified by the functional requirements.

C.5.4.7 Extract, Transform, and Load (ETL)

The Contractor solution shall leverage ICE standard ETL technology for the purpose of batch data movement between data stores. ICE architecture supports the batch movement of data from one location to another for value added purposes only (information must be transformed, reorganized or otherwise enhanced). Data movement (without substantial enhancement) is also supported for purposes of meeting user analytical needs when such activity would clearly impact operations due to the consumption of necessary resources AND operational systems cannot be reasonably tuned or optimized to meet the requirement for data access. Note that real time information exchanges are more frequently handled through services (application tier) and service bus infrastructure.

C.5.4.8 Miscellaneous

The Contractor shall also:

- Develop system user guides, help files, and context-sensitive help information that will be incorporated into the application.
- Follow detailed guidance contained within the Functional Requirements Document regarding system functional requirements and timing for delivery of functionality.
- Utilize the shared ICE OCIO Application Hosting Services (AHS) development and test environments hosted at DHS data center. Otherwise the Contractor must design the application and Development and Test environments in compliance with ICE OCIO AHS such that it can be hosted at the DHS data center. The shared ICE OCIO AHS development and test environments hosted at the DHS data center can be accessed remotely from a Contractor site.

ICE has made significant strides in the modernization of a consolidated application hosting infrastructure. The application hosting infrastructure provides a robust, enterprise-class Java Enterprise Edition (JEE) hosting platform for ICE's hosted applications as well as complimentary capabilities directed toward composite service applications and business process modeling and orchestration. ICE anticipates the use of the following infrastructure in supporting the production version of this service:

- IBM DataPower: The DataPower appliance provides XML processing, transformation and security

- IBM Websphere: The Websphere software suite provides business and application logic services
- Oracle RDBMS: Oracle provides the relational database necessary for the support of data storage and retrieval
- Red Hat Enterprise Linux: Linux provides a highly reliable and secure operating system for the production implementation of application services

In the event that development cannot be fully performed on shared infrastructure, Contractor shall procure necessary hardware (e.g. servers) and software (e.g. database) for use in Development and Test environments which shall be hosted at the Contractor's facility. The Contractor will **not** be required to procure hardware (e.g. servers) or software (e.g. database) for use in the DHS data center's Production or Backup (COOP) hosting environment. The Contractor shall be expected to model and compute the necessary hardware capacities.

C.6 OPTIONAL REQUIREMENTS

Optional Requirement tasks are work assignments, activities, and/or projects that the Government has identified as potential work that may be required under this task order during the period of performance. The Contracting Officer (CO) will inform the Contractor if the Optional Requirement tasks will be exercised.

C.7 REFERENCES

- National Industrial Security Program Operating Manual (NISPOM)
- DHS Management Directive (MD) 4300, *IT Systems Security*
- System Lifecycle Management (SLM) Handbook
- Federal Information Security Management Act (FISMA), November 22, 2002
- Federal Information Technology Security Assessment Framework (FITSAF), November 28, 2000
- Office of Management and Budget (OMB) Circular A-127, *Financial Management Systems*
- OMB Circular A-130, *Management of Federal Information Resources*
- National Institute of Standards and Technology (NIST) Computer Security Resource Center (CSRC)
  - Standards
  - Guidelines
  - Special Publications

- Privacy Act of 1974 (As Amended)
- DHS Management Directives Volume 11000 – Security
- DHS 4300A *Sensitive Systems Handbook*, Version 5.5, September 30, 2007
- DHS 4300B *National Security Systems Handbook*, Version 4.3, September 30, 2007
- DHS 4300C *Sensitive Compartmented Information Systems Handbook*, Version 1.0 February 2008
- DHS Technical Reference Model
- National Institute of Standards and Technology (NIST) Special Publication 800-37, *Guide for the Certification and Accreditation of Federal Information Systems*
- International Information Systems Security Certification Consortium (ISC^2) Standards
- Director of Central Intelligence Directive (DCID) 6/3 *Protecting Sensitive Compartmented Information Within Information Systems* - 05 June 1999

C.8 KEY PERSONNEL

The Government has determined that the Project Manager and Project Leads are key personnel for this task order Key personnel shall be located within the greater Washington, D.C. area (GWA) to enable them to interface with client personnel on a regular basis.

The Project Manager shall possess the technical and leadership skills requirements set forth under the labor categories in the DHS EAGLE contract. In addition to those skills, it is desired that the Project Manager be Project Management Professional (PMP)-certified, and have 8-10 years of IT-related program management experience or have experience managing law enforcement, biometric-capable and/or enterprise-wide systems.

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

C.9 DELIVERABLES AND DELIVERY SCHEDULE

The deliverables identified below are the minimum deliverables for this Task Order and additional deliverables may be required based on the requirement. The Contractor shall provide deliverables associated with the work project, assignments, and activities. The Contractor shall be responsible for providing a log of all deliverables assigned, scheduled, and accomplished to the COTR on a monthly basis with the Task Order Monthly Report.

C.9.1 Deliverable Number 1: Task Area Weekly/Monthly Report

The Contractor shall provide 2 electronic copies of the weekly and monthly status reports. The weekly and cumulative monthly reports shall list each Subtask in the SOW. The status report shall include administrative issues, accomplishments, status of ongoing activities, management issues, recommendations for problem resolution, and upcoming activities. The status report shall identify any completed travel and projects as well as provide planned travel and resources required for the next 30 calendar days. (See Deliverable Matrix)

C.9.2 Deliverable Number 2: Transition Management Plan

The Contractor shall provide 2 copies of the Transition Management Plans (TMP) for the transition in and transition out task described in section 4.5.

C.9.3 Deliverable Number 3: Progress Reports and Program Reviews

Progress reports may be ad hoc requests in addition to the deliverables otherwise defined in this document. They will be specific to the project or an element of the project.

The Contractor shall provide the ICE Program Manager and COTR with 3 copies of the Progress Reports, which shall include, at a minimum, the following topics in the order indicated:

- Title of project
- Associated tasks
- Date Assigned
- Projected Completion Date
- Assigned by
- Reporting period
- Progress of project during the reporting period
- Identification of significant accomplishments or issues noted with details
- Planned solutions of issues
- Schedule - percent or degree completed by task to date, critical path analysis, ability to meet contract schedule, reasons for slippage, and path to recovery
- Cost - analysis of actual costs incurred in relation to budget and progress to date, burn rates, and cost estimate to complete project within budget
- Other as required

Program Reviews (or In Progress Reviews) will occur at least quarterly during the POP of the project. The Program Review is a formal status update of contract administrative, financial, and operational issues.

C.9.4 Deliverable Number 4: Project Plan and Schedule

The Contractor shall deliver 3 copies of the project plan to the Task Manager and COTR 30 days from the start of the Period of Performance (POP) for review. Review comments and edits will be integrated into the Project Plan within 10 calendar days of receipt from the ICE Task Manager or COTR. The project plan will include at a minimum:

- Project Management Plan
- Scope Management Plan
- Work Breakdown Structure
- Work Schedule
- Resource Management Plan
- Milestones
- Risk Management Plan
- Quality Assurance Plan

C.9.5 Deliverable Number 5: Cost/Schedule & Earned Value Management System (EVMS) Report

The Contractor shall use an Earned Value Management System (EVMS) that meets the applicable criteria as defined in the current American National Standards Institute/Electronic Industries Alliance (ANSI/EIA) Standard 748-A, Earned Value Management Systems, originally approved May 19, 1998, first amended in 2002 ("the ANSI/EIA Standard"), and most recently on 9 July 2007 and published as Government Electronic and Information Technology Association's EIA-748-B. Also, contractors must describe how they expect to follow the EVMS and how they will evaluate their compliance with the EVMS system in the contract.

The Contractor shall submit 3 copies of the EVM report monthly to the COTR. The reports must be prepared in sufficient detail to support Office of Management and Budget (OMB) A-11 reporting requirements at Exhibits 53 and 300. Note that ICE requires the use of Earned Value Reporting. The report is due on the 10th business day of each calendar month, starting with the second calendar month after Contract award. The initial report shall cover the first calendar month of Contract performance. Subsequent reports will be provided monthly and shall cover the calendar month that began at the conclusion of the last reported period.

C.9.6 Deliverable Number 6: Quality Control Plan

The Contractor shall provide a Quality Control Plan (QCP). The QCP shall provide details of how the Contractor intends to perform quality control checks, the process for tracking issues, communication strategy, and the quality control measures for all areas and responsibilities of this TO to include but not be limited to all deliverables, all Contract Line Items and work activities, assignments, and projects. The Contractor shall be prepared to address COTR concerns and requirements as well as to include the QCP Report schedule and due date.

The Contractor shall provide the draft QCP to the COTR within 60 calendar days of task order award, for the Government to review. After the COTR provides comments back to the Contractor, the Contractor shall incorporate the comments and provide the final QCP to the COTR and CO within 10 business days.

The Contractor shall deliver three (3) hard copies and one (1) electronic copy of each deliverable to the COTR.

C.9.7 DELIVERABLE MATRIX

DELIVERABLE DESCRIPTION	FRENQUENCY	DATE OF SUBMISSION	COPIES	ICE DISTRUBTION
Weekly Report	Weekly	Monday, close of business, each week	2 (electronic)	Program Manager COTR
Monthly Report	Monthly	15th of the month or first business day prior to the 15th, if it falls on non-business day	2 (electronic)	Program Manager COTR
Transition Plan (In) Final	Once	Within 5 business days after kickoff meeting	2	Program Manager COTR
Transition Plan (Out) Final	Once	120 calendar days prior to the completion of the period of performance of this contract	2	Program Manager COTR
Progress Report	Quarterly	TBD	3	Program Manager COTR CO

DELIVERABLE DESCRIPTION	FRENQUENCY	DATE OF SUBMISSION	COPIES	ICE DISTRUBTION
Project Plan	Once (Initial and as revised)	Due 30 calendar day after award. Final due 10 business days after revisions	2	Program Manger COTR
Cost/Schedule & EVMS Report	Monthly	15th of the month or first business day prior to the 15th, if it falls on non-business day	3	COTR CO
Quality Control Plan	Once	Initial plan- 60 calendar days after date of award Final due 10 days after revisions	3 hardcopies 2 (electronic)	COTR CO

C.10.0 PROJECT PLAN AND SCHEDULE

The project plan shall be delivered to the Task Manager and COTR 30 calendar days from the start of the period of performance (PoP) for review. Review comments and edits will be integrated into the Project Plan within 10 business days of receipt from the Task Manager or COTR. The project plan will include at a minimum:

- Project Management Plan
- Scope Management Plan
- Work Breakdown Structure
- Work Schedule
- Resource Management Plan
- Milestones
- Risk Management Plan
- Quality Assurance Plan

C.11 PROGRESS REPORTS, STATUS REPORTS, & PROGRAM REVIEWS

Progress reports and status reports will be required quarterly in addition to the deliverables otherwise defined in this document. They will be specific to the project or an element of the project.

Program Reviews (or In Progress Reviews) will occur at least quarterly during the POP of the project. The Program Review is a formal status update of contract administrative, financial, and operational issues.

C.12 PRODUCT ACCEPTANCE

ICE will accept or reject deliverables within 15 calendar days after delivery. If rejected, the Contractor will have to make corrections as specified and resubmit the deliverable for review and approval. The Contractor shall also inform the COTR in writing within five (5) business days of the rejection and shall identify what measures have been put into place to reduce future rejection of deliverables.

C.13 GFE AND INFORMATION

The Government will provide laptops, tokens and aircards to the contractor for use. The Contractor shall keep an accurate inventory of the GFE, which can be made available to the Government Task Manager upon request. All information developed by the Contractor under this Task shall be the property of the Federal Government and provided to ICE upon request and at the end of the period of performance.

C.14 PLACE OF PERFORMANCE

Work shall be performed primarily at Contractors facilities in the greater Washington, D.C. area (GWA).

C.15 HOURS OF OPERATION

The Contractor shall cover the normal operational hours of 6:00 am and 6:00 pm Monday through Friday. The Contractor's key staff must be available during the core operational period of 8:30 am to 5:00 pm Monday through Friday. As necessary, the Contractor shall provide support on an on-call basis for after normal operational (working) hours.

C.16 PERIOD OF PERFORMANCE

This requirement will consist of a three (3) month base period plus four 12 month option periods. The base-year period will begin upon task order award.

C.17 SECURITY REQUIREMENTS

ICE has determined that the performance of this contract requires that the Contractor, Subcontractor(s), vendors(s) etc. have access to sensitive ICE information which requires DHS 5C position of public trust adjudication.

C.18 OTHER DIRECT COSTS (ODCs)

ODC TRAVEL

Travel within the Continental U.S. may be required for coordination and data gathering. All travel required by the Contractor shall be approved in advance by the Government

Task Manager and COTR. Travel shall be in accordance with the Federal Travel Regulations (FTR).

The Government COTR must approve all travel costs and a copy of the approval form must be provided to the COTR prior to travel. The Contractor shall submit an estimate to the Government COTR by the 15th day prior to the month for which travel is being requested. Local travel may be required but is not a reimbursable cost under this task order. In addition, the Government COTR must approve all Outside of the Continental United States (OCONUS) travel costs prior to travel. Any foreign travel must be compliant with the DHS policy requiring "country clearance". Country Clearance must be received prior to the start of foreign travel.

APPENDIX A – LIST OF ACRONYMS

ACRIMe System	Alien Criminal Response Information Management
BPEL	Business Process Execution Language
C&A	Certification and Accreditation
CCD	Consular Consolidated Database
COB	Close of Business
CO	Contracting Officer
COOP	Contingency of Operations
COTR	Contracting Officer Technical Representative
COTS	Commercial Off-The-Shelf
CPIC	Capital Planning and Investment Control
CSIRC	Computer Security Incident Response Center
CSRC	Computer Security Resource Center
DCID	Director of Central Intelligence Directive
DHS	Department of Homeland Security
DoJ	Department of Justice
DOS	Department of State
EA	Enterprise Architecture
EIT	Electronic and Information Technology
EOD	Entry on Duty
ESB	Enterprise Service Bus
FAR	Federal Acquisition Regulations
FISMA	Federal Information Security Management Act
FITSAF Framework	Federal Information Tech Security Assessment
FRD	Functional Requirements Document
FTR	Federal Travel Regulations
GFE/GFP	Government Furnished Equipment/Property
GJXDM Model	Global Justice Extensible Markup Language Data
GOTS	Government Off-The-Shelf

HLS	Homeland Security
ICE	Immigration and Customs Enforcement
ICEPIC	ICE Pattern Analysis and Collection System
ISA	Interconnection Security Agreements
ISB	Investigative Systems Branch
ISSM	Information System Security Manager
ISSO	Information Systems Security Officer
ITCR	Information Technology Change Request
LEISP	Law Enforcement Information Sharing Program
LEISS	Law Enforcement Information Sharing Service
LEXS	LEISP Exchange Specifications
MD	Management Directive
NIEM	National Information Exchange Model
NISPOM Manual	National Industrial Security Program Operating
NIST	National Institute of Standards and Technology
O&M	Operations and Maintenance
OAST	Office on Accessible Systems and Technology
OCIO	Office of the Chief Information Officer
OCONUS	Outside of the Continental United States
ODC	Other Direct Cost
OI	Office of Investigations
OIA	Office of International Affairs
OMB	Office of Management and Budget
OPLA	Office of Principal Legal Advisor
OPR	Office of Professional Responsibility
PMP	Project Management Plan
QCP	Quality Control Plan
SCI	Sensitive Compartmented Information
SBU	Sensitive But Unclassified
SDD	Systems Development Division
SEVIS	Student Exchange Visitor System
SLM	System Lifecycle Management

SME	Subject Matter Expert
SOA	Service Oriented Architecture
SOAP	Simple Object Access Protocol
SOW	Statement of Work
SPBP	Significant Public Benefit Parole
TMP	Transition Management Plan
TRM	Technical Reference Model
UAT	User Acceptance Testing
UDDI	Universal Description, Discovery and Integration
UMF	Universal Message Format
USCIS	United States Citizenship and Immigration Services
VSO	Visa Security Officer
VSP	Visa Security Program
WBS	Work Breakdown Structure
WSDL	Web Services Description Language
XML	Extensible Markup Language

Section D: Packaging and Marking

NOT APPLICABLE

THIS PAGE WAS INTENTIONALLY LEFT BLANK

Section E: Inspection and Acceptance

E.1 52.246-4 Inspection of Services—Fixed-Price (1996)

(a) *Definition.* "Services," as used in this clause, includes services performed, workmanship, and material furnished or utilized in the performance of services.

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

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

(d) If the Government performs inspections or tests on the premises of the Contractor or a subcontractor, the Contractor shall furnish, and shall require subcontractors to furnish, at no increase in contract price, all reasonable facilities and assistance for the safe and convenient performance of these duties.

(e) If any of the services do not conform to contract requirements, the Government may require the Contractor to perform the services again in conformity with contract requirements, at no increase in contract amount. When the defects in services cannot be corrected by reperformance, the Government may—
(1) Require the Contractor to take necessary action to ensure that future performance conforms to contract requirements; and
(2) Reduce the contract price to reflect the reduced value of the services performed.

(f) If the Contractor fails to promptly perform the services again or to take the necessary action to ensure future performance in conformity with contract requirements, the Government may—
(1) By contract or otherwise, perform the services and charge to the Contractor any cost incurred by the Government that is directly related to the performance of such service; or
(2) Terminate the contract for default.
(End of clause)

52.462-5 Inspection of Services—Cost-Reimbursement (Apr 1984)

As prescribed in 46.305, insert the following clause in solicitations and contracts for services, or supplies that involve the furnishing of services, when a cost-reimbursement contract is contemplated:

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

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

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

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

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

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

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

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

(2) Terminate the contract for default.

Section F: Deliveries or Performance

F.1 PLACE OF PERFORMANCE/HOURS OF OPERATION

Work shall be performed at the Contractors facility in the Greater Washington Area (GWA). See the Statement of Work, Paragraph C.14 page 33.

F.2 PERIOD OF PERFORMANCE

The period of performance for this requirement is a three (3) month base period plus four (4) 12-month option periods.

F.3 DELIVERY SCHEDULE

Required deliverables and delivery schedules are established in Section C, Statement of Work and determined in coordination with the Contracting Officer's Technical Representative.

Section G: Contract Administration

G.1 Commitment of Government to Award A Contract and Expenditure of Funds

The Contracting Officer is the only individual who can legally commit the Government to the expenditure of public funds in connection with the contract.

G.2 Technical Direction and Surveillance

(a) Performance of the work under this contract shall be subject to the surveillance and written technical direction of the Contracting Officer's Technical Representative (COTR), who shall be specifically appointed by the Contracting Officer in writing. Technical direction is defined as a directive to the Contractor which approves approaches, solutions, designs, or refinements; fills in details or otherwise completes the general description of work of documentation items; shifts emphasis among work areas or tasks; or otherwise furnishes guidance to the Contractor. Technical direction includes the process of conducting inquiries, requesting studies, or transmitting information or advice by the COTR, regarding matters within the general tasks and requirements in Section C of this contract.

(b) The COTR does not have the authority to, and shall not, issue any technical direction which:

(1) Constitutes an assignment of additional work outside the Performance Work Statement;

(2) Constitutes a change as defined in the contract clause entitled "Changes";

(3) In any manner causes an increase or decrease in the total estimated contract cost, the fixed fee (if any), or the time required for contract performance;

(4) Changes any of the expressed terms, conditions, or specifications of the contract; or
(5) Interferes with the Contractor's right to perform the specifications of the contract.

(c) All technical directions shall be issued in writing by the COTR via e-mail

(d) The Contractor shall proceed promptly with the performance of technical directions duly issued by the COTR in the manner prescribed by this clause and within his/her authority under the provisions of this clause. Any instruction or direction by the COTR which falls within one, or more, of the categories defined in (b)(1) through (5) above, shall cause the Contractor to notify the Contracting Officer in writing within five (5) working days after receipt of any such instruction or direction and shall request the Contracting Officer to modify the contract accordingly. Upon receiving the notification from the Contractor, the Contracting Officer shall either issue an appropriate contract modification within a reasonable time or advise the Contractor in writing within thirty (30) days after receipt of the Contractor's Letter that:

(1) the technical direction is rescinded in its entirety; or

(2) the technical direction is within the scope of the contract, does not constitute a change under the "Changes" clause of the contract and that the Contractor should continue with the performance of the technical direction.

(e) A failure of the Contractor and Contracting Officer to agree that the technical direction is within scope of the contract, or a failure to agree upon the contract action to be taken with respect thereto shall be subject to the provisions of the "Disputes" clause of this contract.

(f) Any action(s) taken by the Contractor in response to any direction given by any person other than the Contracting Officer or the Project Officer whom the Contracting Officer shall appoint shall be at the Contractor's risk.

G.3 Invoices

Invoice procedures for invoice submittal (Reference EAGLE IDIQ Contract Section G, Contract Administration Data, and Section I, Contract Clauses)

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

a.) By mail

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

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

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

Invoices submitted by other than these three methods will be returned. Contractor Taxpayer Identification Number (TIN) must be registered in the Central Contractor Registration (http://www.ccr.gov) prior to award and shall be notated on every invoice submitted to ICE/OAQ. The ICE program office identified in the delivery order/contract shall also be notated on every invoice.

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

An invoice must include:

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

Invoices without the above information may be returned for resubmission.

3. The Contractor shall also submit the invoice electronically to the following people:

Contract Specialist: Kimberlee Brown

Contracting Officer's Technical Representative: Scott A. Johnston

G.4 Designation of Contraction Officer's Technical Representative (COTR)

For the purpose of this contract, the Contracting Officer's Technical Representative shall be: Scott A. Johnston.

G.5 The Following Contact Information Is Provided:

Task Order Contract Specialist:

Kimberlee Brown
Contract Specialist
USICE Office of Acquisition Management
801 I St. N.W.
8th Floor
Washington, DC 20536

Email: [redacted]
Office Phone: 202-732-[redacted]

Task Order Contracting Officer:

Maxine Edwards
Contracting Officer
USICE Office of Acquisition Management
801 I St. N.W.
8th Floor
Washington, DC 20536

Email: [redacted]
Office Phone: 202-732-[redacted]

Task Order Contracting Officer Technical Representative:

Scott A. Johnston
Program Manager LEISS
DHS/ICE OCIO
SDD Investigations Branch
801 I St. N.W.
7th Floor
Washington, DC 20536

Email: [redacted]
Blackberry Number: (202) 306-[redacted]
Fax: (305) 675-[redacted]

Finance Office/Invoice Address:

DHS ICE
Burlington Finance Center (BFC)
P.O. Box 1620
Williston, VT 05495-1620
Attn: ICE/OCIO/SDD invoice

Section H: Special Contracting Requirements

H.1 Accessibility Requirements

Section 508 of the Rehabilitation Act, as amended by the Workforce Investment Act of 1998 (P.L. 105-220) requires that when Federal agencies develop, procure, maintain, or use electronic and information technology, they must ensure that it is accessible to people with disabilities. Federal employees and members of the public who have disabilities must have equal access to and use of information and data that is comparable to that enjoyed by non-disabled Federal employees and members of the public.

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

- 36 CFR 1194.21 – Software Applications and Operating Systems, applies to all EIT software applications and operating systems procured or developed under this work statement including but not limited to GOTS and COTS software. In addition, this standard is to be applied to Web-based applications when needed to fulfill the functional performance criteria. This standard also applies to some Web-based applications as described within 36 CFR 1194.22.
- 36 CFR 1194.22 – Web-based Intranet and Internet Information and Applications, applies to all Web-based deliverables, including documentation and reports procured or developed under this work statement. When any Web application uses a dynamic (non-static) interface, embeds custom user control(s), embeds video or multimedia, uses proprietary or technical approaches such as, but not limited to, Flash or Asynchronous JavaScript and XML (AJAX) then "1194.21 Software" standards also apply to fulfill functional performance criteria.
- 36 CFR 1194.23 – Telecommunications Products, applies to all telecommunications products including end-user interfaces such as telephones and non end-user interfaces such as switches, circuits, etc. that are procured, developed or used by the Federal Government.
- 36 CFR 1194.24 – Video and Multimedia Products, applies to all video and multimedia products that are procured or developed under this work statement. Any video or multimedia presentation shall also comply with the software standards (1194.21) when the presentation is through the use of a Web or Software application interface having user controls available. This standard applies to any training videos provided under this work statement.
- 36 CFR 1194.31 – Functional Performance Criteria applies to all EIT deliverables regardless of delivery method. All EIT deliverable shall use technical standards, regardless of technology, to fulfill the functional performance criteria.
- 36 CFR 1194.41 – Information Documentation and Support, applies to all documents, reports, as well as help and support services. To ensure that

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

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

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

  When applying this standard, all procurements of EIT shall have documentation of market research that identify a list of products or services that first meet the agency business needs, 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.

H.2 IT Security Requirements

H.2.1 General

To ensure the security of the DHS/ICE information in their charge, ICE Contractors and Sub-contractors must adhere to the same computer security rules and regulations as Federal Government employees unless an exception to policy is agreed to by the prime Contractors, ICE ISSM and Contracting Officer and detailed in the contract. Non-DHS

Federal employees or Contractors who fail to comply with DHS/ICE security policies are subject to having their access to DHS/ICE IT systems and facilities terminated, whether or not the failure results in criminal prosecution. The DHS Rules of Behavior document applies to DHS/ICE support Contractors and Sub-contractors.

H2.2 Security Policy References Clause

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

- DHS 4300A, Sensitive Systems Policy Directive
- DHS 4300A, IT Security Sensitive Systems Handbook
- ICE Directive, IT Security Policy for SBU Systems

H.2.3 Contractor Information Systems Security Officer (ISSO) Point of Contact Clause

The Contractor must appoint and submit name to ICE ISSM for approval, via the ICE COTR, of a qualified individual to act as ISSO to interact with ICE personnel on any IT security matters.

H.2.4 Protection of Sensitive Information

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

H.2.5 Information Technology Security Program

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

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

- Certification and Accreditation and FISMA compliance (C&A) of Systems containing, processing or transmitting of DHS/ICE data
- Training and Awareness for Contractor personnel
- Security Incident Reporting
- Contingency Planning
- Security Reviews
- Contract Closeout Actions

H.2.6 Handling of Sensitive Information and IT Resources

The Contractor shall protect DHS/ICE sensitive information and all government provided and Contractor-owned IT systems used to store or process DHS/ICE sensitive information. The Contractor shall adhere to the following requirements for handling sensitive information:

- **Media Protection**. The Contractor shall ensure that all hardcopy and electronic media (including backup and removable media) that contain DHS sensitive information are appropriately marked and secured when not in use. Any sensitive information stored on media to be surplused, transferred to another individual, or returned to the manufacturer shall be purged from the media before disposal. Disposal shall be performed using DHS/ICE approved sanitization methods. The Contractor shall establish and implement procedures to ensure sensitive information cannot be accessed or stolen. These procedures shall address the handling and protection of paper and electronic outputs from systems (computers, printers, faxes, copiers) and the transportation and mailing of sensitive media.)
- **Access Control.** The Contractor shall control user access to DHS/ICE sensitive information based on positive user identification, authentication and authorization (Roles and Rules based) mechanisms. Access control measures employed shall provide protection from unauthorized alternation, loss, unavailability, or disclosure of information. The Contractor shall ensure its personnel are granted the most restrictive set of access privileges needed for performance of authorized tasks. The Contractor shall divide and separate duties and responsibilities of critical IT functions to different individuals so that no individual has all necessary authority or systems access privileges needed to disrupt or corrupt a critical process.
- **Auditing.** The Contractor shall ensure that its Contractor-owned IT systems used to store or process DHS/ICE sensitive information maintain an audit trail sufficient to reconstruct security relevant events. Audit trails shall include the identity of each person and device accessing or attempting to access the system, the time and date of the access and the log-off time, activities that might modify, bypass, or negate security safeguards, and security-relevant actions associated with processing. The Contractor shall periodically review audit logs and ensure

that audit trails are protected from modification, authorized access, or destruction and are retained and regularly backed up.

- **Network Security.** The Contractor shall monitor its networks for security events and employ intrusion detection systems capable of detecting inappropriate, incorrect, or malicious activity. Any interconnections between Contractor-owned IT systems that process or store DHS/ICE sensitive information and IT systems not controlled by DHS/ICE shall be established through controlled interfaces and documented through formal Interconnection Security Agreements (ISA). The Contractor shall employ boundary protection devices to enforce access control between networks, including Internet and extranet access. The Contractor shall ensure its e-mail systems are secure, properly configured, and that network protection mechanisms implemented in accordance with DHS/ICE requirements. The Contractor shall conduct periodic vulnerability assessments and tests on its IT systems containing DHS/ICE sensitive information to identify security vulnerabilities. The results, of this information, will be provided to the ICE OCIO for review and to coordinate remediation plans and actions.
- DHS employees and contractors shall not transmit sensitive DHS/ICE information to any personal e-mail account that is not authorized to receive it.
- **Rules of Behavior.** The Contractor shall develop and enforce Rules of Behavior for Contractor-owned IT systems that process or store DHS/ICE sensitive information. These Rules of Behavior must meet or exceed the DHS/ICE rules of behavior.
- The Contractor shall adhere to the policy and guidance contained in the DHS/ICE reference documents.

H.3 Training and Awareness

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

- Any Contractor personnel who are appointed as ISSO, Assistant ISSOs, or other position with IT security responsibilities, i.e., System/LAN Database administrators, system analyst and programmers may be required to attend and participate in the annual DHS Security Conference.

H.4 Certification and Accreditation (C&A) and FISMA compliance

The Contractor shall ensure that any Contractor-owned systems that process, store, transmit or access DHS/ICE information shall comply with the DHS/ICE C&A and FISMA requirements.

Any work on developing, maintaining or modifying DHS/ICE systems must be done to ensure that DHS/ICE systems are in compliance with the C&A and FISMA requirements. The Contractor must ensure that the necessary C&A and FISMA compliance requirements are being effectively met prior to the System or application's release into Production (this also includes pilots). The Contractor shall use the DHS provided tools for C&A and FISMA compliance and reporting requirements.

H.4.1 Security Incident Reporting

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

H.4.2 Contingency Planning

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

H.4.3 Security Review and Reporting

- The Contractor shall include security as an integral element in the management of this contract. The Contractor shall conduct reviews and report the status of the implementation and enforcement of the security requirements contained in this contract and identified references.
- The Government may elect to conduct periodic reviews to ensure that the security requirements contained in this contract are being implemented and enforced. The Contractor shall afford DHS/ICE, including the Office of

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

H.5 Use of Government Equipment

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

H.6 Contract Closeout

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

H.6.1 Personnel Security

- DHS/ICE does not permit the use of non U.S. Citizens in the performance of this contract or to access DHS/ICE systems or information
- All Contractor personnel (including Sub-contractor personnel) must have favorably adjudicated background investigations commensurate with the sensitivity level of the position held before being granted access to DHS/ICE sensitive information.
- The Contractor shall ensure all Contractor personnel are properly submitted for appropriate clearances.
- The Contractor shall ensure appropriate controls have been implemented to prevent Contractor personnel from obtaining access to DHS/ICE sensitive information before a favorably adjudicated background investigation has been completed and appropriate clearances have been issued. At the option of the government, interim access may be granted pending completion of a pre-employment check. Final access may be granted only upon favorable completion of an appropriate background investigation based on the risk level assigned to this contract by the Contracting Officer.

- The Contractor shall ensure its personnel have a validated need to access DHS/ICE sensitive information and are granted the most restrictive set of access privileges needed for performance of authorized tasks.
- The Contractor shall ensure that its personnel comply with applicable Rules of Behavior for all DHS/ICE and Contractor-owned IT systems to which its personnel have been granted access privileges.
- The Contractor shall implement procedures to ensure that system access privileges are revoked for Contractor personnel whose employment is terminated or who are reassigned to other duties and no longer require access to DHS/ICE sensitive information.
- The Contractor shall conduct exit interviews to ensure that Contractor personnel who no longer require access to DHS/ICE sensitive information understand their obligation not to discuss or disclose DHS/ICE sensitive information to which they were granted access under this contract.

H.7 Physical Security

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

H.8 Contractor Personnel Security Requirements

H.8.1 General

ICE has determined that the performance of this contract requires that the Contractor, Subcontractor(s), vendors(s) etc. have access to sensitive ICE information which requires DHS 5C position of public trust adjudication.

H.8.2 Suitability Determination

ICE shall have and exercise full control over granting, denying, withholding or terminating unescorted government facility and/or sensitive Government information access for Contractor employees, based upon the results of a background investigation. ICE 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 ICE, at any time during the term of the purchase order. No employee of the Contractor shall be allowed unescorted access to a Government facility without a favorable EOD decision or suitability determination by the Security Office. Contract employees assigned to the contract not needing access to sensitive ICE information or recurring access to ICE facilities will not be subject to security suitability screening.

H.8.3 Background Investigations

Contract employees (to include applicants, temporaries, part-time and replacement employees) under this contract, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the purchase order. The results of the position sensitivity analysis shall identify the appropriate background investigation to be conducted. All background investigations will be processed through the Security Office. Prospective Contractor employees shall submit the following completed forms to the Security Office through the COTR no less than thirty (30) days before the starting date of the contract or thirty (30) days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

- Standard Form 85P, "Questionnaire for Public Trust Positions"
- FD Form 258, "Fingerprint Card" (2 copies)
- Foreign National Relatives or Associates Statement
- Form DOJ-555, "Disclosure and Authorization Pertaining to Consumer Reports pursuant to the Fair Credit Reporting Act.

ICE will provide required forms, at the time of award of the contract. The Security Office will accept only completed packages. Specific instructions on submission of packages will be provided upon award of the contract.

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

In the interest of limiting access to potentially sensitive information and systems, ICE will consider only U.S. Citizens and Legal Permanent Residents for employment on this contract.

H.8.4 Continued Eligibility

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

The Security Office may require drug screening for probable cause at any time and/ or when the Contractor independently identifies circumstances where probable cause exists.

ICE 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 Department of Justice (DOJ) standards of conduct, 5 CFR 2635 and 5 CFR 3801, or whom ICE determines to present a risk of compromising sensitive Government information to which he or she would have access under this purchase order.

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

The Security Office must be notified of all terminations/resignations within five (5) days of occurrence. The Contractor shall return any expired ICE 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 individuals to whom issued, the last known location and disposition of the pass or card.

H.8.5 Employment Eligibility

The Contractor must agree that each employee working on this purchase order will have a Social Security Card issued and approved by the Social Security Administration. The Contractor shall be responsible to the Government for acts and omissions of his own employees and for any Subcontractor(s) and their employees. Subject to existing law, regulations and/or other provisions of this purchase order, illegal or undocumented aliens will not be employed by the Contractor, or with this purchase order. The Contractor shall ensure that this provision is expressly incorporated into any and all Subcontracts or subordinate agreements issued in support of this purchase order.

H.8.6 Security Management

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual shall 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 of this purchase order. Should the COTR determine that the Contractor is not complying with the security requirements of this contract; the Contractor shall be informed in writing by the CO of the proper action to be taken in order to effect compliance with such requirements.

H.8.7 TAIS Clearance

When sensitive Government information is processed on Telecommunications and Automated Information Systems (TAIS), the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DOJ Order 2640.2C, TAIS Security.

H.9 Personal Service

ICE has determined the requirements as outlined in this SOW are in the best interest of the Government, economic and other factors considered, and is not being used to procure personal services prohibited by the Federal Acquisition Regulation (FAR) Part 37.104 entitled "Personal Services Contract."

H.10 DHS Enterprise Architecture Compliance

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

- All developed solutions and requirements shall be compliant with the HLS EA.
- All IT hardware or software shall be compliant with the HLS EA Technology Reference Model Standards and Products Profile.
- All data assets, information exchanges and data standards, whether adopted or developed, shall be submitted to the DHS Enterprise Data Management Office for review and insertion into the DHS Data Reference Model.
- In compliance with Office of Management and Budget (OMB) mandates, all network hardware shall be IPv6 compatible without modification, upgrade, or replacement.

H.11 Transition

Upon award, if applicable, there will be a transition period of 120 days from the incumbent Contractor to the newly awarded Contractor. Both Contractors shall complete technical Transition Management Plans (TMPs) within 120 days after the contract award. The technical activities, which shall be included as part of the technical transition, consist of transition plans for the:

- Inventory and orderly transfer of all GFE/GFP, software and licenses
- Transfer of documentation currently in process at the time of TO award
- Transfer of all Software coding in process at the time of TO award
- Establishment of a facility for housing hardware/software, if any
- Coordinating the body of work with the current Contractor and turnover of tasking, staffing, etc.
- Review and coordination of changes from a project's TMP to include the closure of gaps within the software
- Work with the infrastructure ICE receiving organizations in the identification and initial resolution/mitigation of all Infrastructure gaps according to the TMP
- Incorporate readiness feedback from discussions with receiving organizations
- Discuss and analyze high level project infrastructure impacts with project and receiving organization managers to capture operational concerns

The Contractor's transition plan shall be approved by DHS, ICE and shall contain a milestone schedule of events and system turnovers. The TMP shall transition systems with no disruption in operational services. The Contractor shall provide the transition management plan 15 days after contract award. To ensure the necessary continuity of services and to maintain the current level of support, DHS, ICE will retain services of the incumbent Contractor for the transition period, if required.

At the completion of the period of performance of this contract, the Contractor shall fully support the transition of Systems Development requirements to the successor. Responsibilities include supporting all of the activities listed above by making available personnel and documentation required to facilitate a successful transition.

Upon completion of the authorized period of performance for this contract including exercised options, the Contracting Officer shall issue a modification to authorize and fund the transition activity of the outgoing Contractor.

Section I: Contract Clauses

Task Order Terms and Conditions

This Task Order will be issued in accordance with the Terms and Conditions of the Enterprise Acquisition Gateway for Leading-Edge Solutions (Eagle) Contract.

Contract Clauses

I.1 52.216-7 Allowable Cost and Payment (Dec 2002)

(a) Invoicing.

(1) The Government will make payments to the Contractor when requested as work progresses, but (except for small business concerns) not more often than once every 2 weeks, in amounts determined to be allowable by the Contracting Officer in accordance with Federal Acquisition Regulation (FAR) Subpart 31.2 in effect on the date of this contract and the terms of this contract. The Contractor may submit to an authorized representative of the Contracting Officer, in such form and reasonable detail as the representative may require, an invoice or voucher supported by a statement of the claimed allowable cost for performing this contract.

(2) Contract financing payments are not subject to the interest penalty provisions of the Prompt Payment Act. Interim payments made prior to the final payment under the contract are contract financing payments, except interim payments if this contract contains Alternate I to the clause at 52.232-25.

(3) The designated payment office will make interim payments for contract financing on the **30th** day after the designated billing office receives a proper payment request. In the event that the Government requires an audit or other review of a specific payment request to ensure compliance with the terms and conditions of the contract, the designated payment office is not compelled to make payment by the specified due date.

(b) Reimbursing costs.

(1) For the purpose of reimbursing allowable costs (except as provided in paragraph (b)(2) of this clause, with respect to pension, deferred profit sharing, and employee stock ownership plan contributions), the term "costs" includes only—

(i) Those recorded costs that, at the time of the request for reimbursement, the Contractor has paid by cash, check, or other form of actual payment for items or services purchased directly for the contract;

(ii) When the Contractor is not delinquent in paying costs of contract performance in the ordinary course of business, costs incurred, but not necessarily paid, for—

(A) Supplies and services purchased directly for the contract and associated financing payments to subcontractors, provided payments determined due will be made—

(1) In accordance with the terms and conditions of a subcontract or invoice; and

(2) Ordinarily within 30 days of the submission of the Contractor's payment request to the Government;

(B) Materials issued from the Contractor's inventory and placed in the production process for use on the contract;

(C) Direct labor;

(D) Direct travel;

(E) Other direct in-house costs; and

(F) Properly allocable and allowable indirect costs, as shown in the records maintained by the Contractor for purposes of obtaining reimbursement under Government contracts; and

(iii) The amount of financing payments that have been paid by cash, check, or other forms of payment to subcontractors.

(2) Accrued costs of Contractor contributions under employee pension plans shall be excluded until actually paid unless—

(i) The Contractor's practice is to make contributions to the retirement fund quarterly or more frequently; and

(ii) The contribution does not remain unpaid 30 days after the end of the applicable quarter or shorter payment period (any contribution remaining unpaid shall be excluded from the Contractor's indirect costs for payment purposes).

(3) Notwithstanding the audit and adjustment of invoices or vouchers under paragraph (g) of this clause, allowable indirect costs under this contract shall be obtained by applying indirect cost rates established in accordance with paragraph (d) of this clause.

(4) Any statements in specifications or other documents incorporated in this contract by reference designating performance of services or furnishing of materials at the Contractor's expense or at no cost to the Government shall be disregarded for purposes of cost-reimbursement under this clause.

(c) *Small business concerns.* A small business concern may receive more frequent payments than every 2 weeks.

(d) Final indirect cost rates.

(1) Final annual indirect cost rates and the appropriate bases shall be established in accordance with Subpart 42.7 of the Federal Acquisition Regulation (FAR) in effect for the period covered by the indirect cost rate proposal.

(2)(i) The Contractor shall submit an adequate final indirect cost rate proposal to the Contracting Officer (or cognizant Federal agency official) and auditor within the 6-month period following the expiration of each of its fiscal years. Reasonable extensions, for

exceptional circumstances only, may be requested in writing by the Contractor and granted in writing by the Contracting Officer. The Contractor shall support its proposal with adequate supporting data.

(ii) The proposed rates shall be based on the Contractor's actual cost experience for that period. The appropriate Government representative and the Contractor shall establish the final indirect cost rates as promptly as practical after receipt of the Contractor's proposal.

(3) The Contractor and the appropriate Government representative shall execute a written understanding setting forth the final indirect cost rates. The understanding shall specify (i) the agreed-upon final annual indirect cost rates, (ii) the bases to which the rates apply, (iii) the periods for which the rates apply, (iv) any specific indirect cost items treated as direct costs in the settlement, and (v) the affected contract and/or subcontract, identifying any with advance agreements or special terms and the applicable rates. The understanding shall not change any monetary ceiling, contract obligation, or specific cost allowance or disallowance provided for in this contract. The understanding is incorporated into this contract upon execution.

(4) Failure by the parties to agree on a final annual indirect cost rate shall be a dispute within the meaning of the Disputes clause.

(5) Within 120 days (or longer period if approved in writing by the Contracting Officer) after settlement of the final annual indirect cost rates for all years of a physically complete contract, the Contractor shall submit a completion invoice or voucher to reflect the settled amounts and rates.

(6)(i) If the Contractor fails to submit a completion invoice or voucher within the time specified in paragraph (d)(5) of this clause, the Contracting Officer may—

(A) Determine the amounts due to the Contractor under the contract; and

(B) Record this determination in a unilateral modification to the contract.

(ii) This determination constitutes the final decision of the Contracting Officer in accordance with the Disputes clause.

(e) *Billing rates.* Until final annual indirect cost rates are established for any period, the Government shall reimburse the Contractor at billing rates established by the Contracting Officer or by an authorized representative (the cognizant auditor), subject to adjustment when the final rates are established. These billing rates—

(1) Shall be the anticipated final rates; and

(2) May be prospectively or retroactively revised by mutual agreement, at either party's request, to prevent substantial overpayment or underpayment.

(f) *Quick-closeout procedures.* Quick-closeout procedures are applicable when the conditions in FAR 42.708(a) are satisfied.

(g) *Audit.* At any time or times before final payment, the Contracting Officer may have the Contractor's invoices or vouchers and statements of cost audited. Any payment may be—

(1) Reduced by amounts found by the Contracting Officer not to constitute allowable costs; or

(2) Adjusted for prior overpayments or underpayments.

(h) Final payment.

(1) Upon approval of a completion invoice or voucher submitted by the Contractor in accordance with paragraph (d)(5) of this clause, and upon the Contractor's compliance with all terms of this contract, the Government shall promptly pay any balance of allowable costs and that part of the fee (if any) not previously paid.

(2) The Contractor shall pay to the Government any refunds, rebates, credits, or other amounts (including interest, if any) accruing to or received by the Contractor or any assignee under this contract, to the extent that those amounts are properly allocable to costs for which the Contractor has been reimbursed by the Government. Reasonable expenses incurred by the Contractor for securing refunds, rebates, credits, or other amounts shall be allowable costs if approved by the Contracting Officer. Before final payment under this contract, the Contractor and each assignee whose assignment is in effect at the time of final payment shall execute and deliver—

(i) An assignment to the Government, in form and substance satisfactory to the Contracting Officer, of refunds, rebates, credits, or other amounts (including interest, if any) properly allocable to costs for which the Contractor has been reimbursed by the Government under this contract; and

(ii) A release discharging the Government, its officers, agents, and employees from all liabilities, obligations, and claims arising out of or under this contract, except—

(A) Specified claims stated in exact amounts, or in estimated amounts when the exact amounts are not known;

(B) Claims (including reasonable incidental expenses) based upon liabilities of the Contractor to third parties arising out of the performance of this contract; provided, that the claims are not known to the Contractor on the date of the execution of the release, and that the Contractor gives notice of the claims in writing to the Contracting Officer within 6 years following the release date or notice of final payment date, whichever is earlier; and

(C) Claims for reimbursement of costs, including reasonable incidental expenses, incurred by the Contractor under the patent clauses of this contract, excluding, however, any expenses arising from the Contractor's indemnification of the Government against patent liability.

I.2 52.216-8 Fixed Fee (Mar 1997)

(a) The Government shall pay the Contractor for performing this contract the fixed fee specified in the Schedule.

(b) Payment of the fixed fee shall be made as specified in the Schedule; provided that after payment of 85 percent of the fixed fee, the Contracting Officer may withhold further payment of fee until a reserve is set aside in an amount that the Contracting Officer considers necessary to protect the Government's interest. This reserve shall not exceed 15 percent of the total fixed fee or $100,000, whichever is less. The Contracting Officer shall release 75 percent of all fee withholds under this contract after receipt of the certified final indirect cost rate proposal covering the year of physical completion of this contract, provided the Contractor has satisfied all other contract terms and conditions, including the submission of the final patent and royalty reports, and is not delinquent in submitting final vouchers on prior years' settlements. The Contracting Officer may release up to 90 percent of the fee withholds under this contract based on the Contractor's past performance related to the submission and settlement of final indirect cost rate proposals.

I.3 52.217-8 Option to Extend Services (Nov 1999)

The Government may require continued performance of any services within the limits and at the rates specified in the contract. These rates may be adjusted only as a result of revisions to prevailing labor rates provided by the Secretary of Labor. The option provision may be exercised more than once, but the total extension of performance hereunder shall not exceed 6 months. The Contracting Officer may exercise the option by written notice to the Contractor within 15 days before the contract expires.

I.4 52.217-9 Option to Extend the Term of the Contract (Mar 2000)

(a) The Government may extend the term of this contract by written notice to the Contractor within 30 days before the contract expires; 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.

I.5 52.227-14 Rights in Data—General (Dec 2007)

(a) *Definitions.* As used in this clause—

"Computer database" or "database means" a collection of recorded information in a form capable of, and for the purpose of, being stored in, processed, and operated on by a computer. The term does not include computer software.

"Computer software"—

(1) Means

(i) Computer programs that comprise a series of instructions, rules, routines, or statements, regardless of the media in which recorded, that allow or cause a computer to perform a specific operation or series of operations; and

(ii) Recorded information comprising source code listings, design details, algorithms, processes, flow charts, formulas, and related material that would enable the computer program to be produced, created, or compiled.

(2) Does not include computer databases or computer software documentation.

"Computer software documentation" means owner's manuals, user's manuals, installation instructions, operating instructions, and other similar items, regardless of storage medium, that explain the capabilities of the computer software or provide instructions for using the software.

"Data" means recorded information, regardless of form or the media on which it may be recorded. The term includes technical data and computer software. The term does not include information incidental to contract administration, such as financial, administrative, cost or pricing, or management information.

"Form, fit, and function data" means data relating to items, components, or processes that are sufficient to enable physical and functional interchangeability, and data identifying source, size, configuration, mating and attachment characteristics, functional characteristics, and performance requirements. For computer software it means data identifying source, functional characteristics, and performance requirements but specifically excludes the source code, algorithms, processes, formulas, and flow charts of the software.

"Limited rights" means the rights of the Government in limited rights data as set forth in the Limited Rights Notice of paragraph (g)(3) if included in this clause.

"Limited rights data" means data, other than computer software, that embody trade secrets or are commercial or financial and confidential or privileged, to the extent that such data pertain to items, components, or processes developed at private expense, including minor modifications.

"Restricted computer software" means computer software developed at private expense and that is a trade secret, is commercial or financial and confidential or

privileged, or is copyrighted computer software, including minor modifications of the computer software.

"Restricted rights," as used in this clause, means the rights of the Government in restricted computer software, as set forth in a Restricted Rights Notice of paragraph (g) if included in this clause, or as otherwise may be provided in a collateral agreement incorporated in and made part of this contract, including minor modifications of such computer software.

"Technical data" means recorded information (regardless of the form or method of the recording) of a scientific or technical nature (including computer databases and computer software documentation). This term does not include computer software or financial, administrative, cost or pricing, or management data or other information incidental to contract administration. The term includes recorded information of a scientific or technical nature that is included in computer databases (See 41 U.S.C. 403(8)).

"Unlimited rights" means the rights of the Government to use, disclose, reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, in any manner and for any purpose, and to have or permit others to do so.

(b) Allocation of rights.

(1) Except as provided in paragraph (c) of this clause, the Government shall have unlimited rights in—

(i) Data first produced in the performance of this contract;

(ii) Form, fit, and function data delivered under this contract;

(iii) Data delivered under this contract (except for restricted computer software) that constitute manuals or instructional and training material for installation, operation, or routine maintenance and repair of items, components, or processes delivered or furnished for use under this contract; and

(iv) All other data delivered under this contract unless provided otherwise for limited rights data or restricted computer software in accordance with paragraph (g) of this clause.

(2) The Contractor shall have the right to—

(i) Assert copyright in data first produced in the performance of this contract to the extent provided in paragraph (c)(1) of this clause;

(ii) Use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, unless provided otherwise in paragraph (d) of this clause;

(iii) Substantiate the use of, add, or correct limited rights, restricted rights, or copyright notices and to take other appropriate action, in accordance with paragraphs (e) and (f) of this clause; and

(iv) Protect from unauthorized disclosure and use those data that are limited rights data or restricted computer software to the extent provided in paragraph (g) of this clause.

(c) Copyright—

(1) Data first produced in the performance of this contract.

(i) Unless provided otherwise in paragraph (d) of this clause, the Contractor may, without prior approval of the Contracting Officer, assert copyright in scientific and technical articles based on or containing data first produced in the performance of this contract and published in academic, technical or professional journals, symposia proceedings, or similar works. The prior, express written permission of the Contracting Officer is required to assert copyright in all other data first produced in the performance of this contract.

(ii) When authorized to assert copyright to the data, the Contractor shall affix the applicable copyright notices of 17 U.S.C. 401 or 402, and an acknowledgment of Government sponsorship (including contract number).

(iii) For data other than computer software, the Contractor grants to the Government and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly by or on behalf of the Government. For computer software, the Contractor grants to the Government, and others acting on its behalf, a paid-up, nonexclusive, irrevocable, worldwide license in such copyrighted computer software to reproduce, prepare derivative works, and perform publicly and display publicly (but not to distribute copies to the public) by or on behalf of the Government.

(2) *Data not first produced in the performance of this contract.* The Contractor shall not, without the prior written permission of the Contracting Officer, incorporate in data delivered under this contract any data not first produced in the performance of this contract unless the Contractor—

(i) Identifies the data; and

(ii) Grants to the Government, or acquires on its behalf, a license of the same scope as set forth in paragraph (c)(1) of this clause or, if such data are restricted computer software, the Government shall acquire a copyright license as set forth in paragraph (g)(4) of this clause (if included in this contract) or as otherwise provided in a collateral agreement incorporated in or made part of this contract.

(3) *Removal of copyright notices.* The Government will not remove any authorized copyright notices placed on data pursuant to this paragraph (c), and will include such notices on all reproductions of the data.

(d) *Release, publication, and use of data.* The Contractor shall have the right to use, release to others, reproduce, distribute, or publish any data first produced or specifically used by the Contractor in the performance of this contract, except—

(1) As prohibited by Federal law or regulation (*e.g.*, export control or national security laws or regulations);

(2) As expressly set forth in this contract; or

(3) If the Contractor receives or is given access to data necessary for the performance of this contract that contain restrictive markings, the Contractor shall treat the data in accordance with such markings unless specifically authorized otherwise in writing by the Contracting Officer.

(e) Unauthorized marking of data.

(1) Notwithstanding any other provisions of this contract concerning inspection or acceptance, if any data delivered under this contract are marked with the notices specified in paragraph (g)(3) or (g) (4) if included in this clause, and use of the notices is not authorized by this clause, or if the data bears any other restrictive or limiting markings not authorized by this contract, the Contracting Officer may at any time either return the data to the Contractor, or cancel or ignore the markings. However, pursuant to 41 U.S.C. 253d, the following procedures shall apply prior to canceling or ignoring the markings.

(i) The Contracting Officer will make written inquiry to the Contractor affording the Contractor 60 days from receipt of the inquiry to provide written justification to substantiate the propriety of the markings;

(ii) If the Contractor fails to respond or fails to provide written justification to substantiate the propriety of the markings within the 60-day period (or a longer time approved in writing by the Contracting Officer for good cause shown), the Government shall have the right to cancel or ignore the markings at any time after said period and the data will no longer be made subject to any disclosure prohibitions.

(iii) If the Contractor provides written justification to substantiate the propriety of the markings within the period set in paragraph (e)(1)(i) of this clause, the Contracting Officer will consider such written justification and determine whether or not the markings are to be cancelled or ignored. If the Contracting Officer determines that the markings are authorized, the Contractor will be so notified in writing. If the Contracting Officer determines, with concurrence of the head of the contracting activity, that the markings are not authorized, the Contracting Officer will furnish the Contractor a written determination, which determination will become the final agency decision regarding the appropriateness of the markings unless the Contractor files suit in a court of competent jurisdiction within 90 days of receipt of the Contracting Officer's decision. The Government will continue to abide by the markings under this paragraph (e)(1)(iii) until final resolution of the matter either by the Contracting Officer's determination becoming final (in which instance the Government will thereafter have the right to cancel or ignore the markings at any time and the data will no longer be made subject to any disclosure prohibitions), or by final disposition of the matter by court decision if suit is filed.

(2) The time limits in the procedures set forth in paragraph (e)(1) of this clause may be modified in accordance with agency regulations implementing the Freedom of Information Act (5 U.S.C. 552) if necessary to respond to a request thereunder.

(3) Except to the extent the Government's action occurs as the result of final disposition of the matter by a court of competent jurisdiction, the Contractor is not precluded by paragraph (e) of the clause from bringing a claim, in accordance with the Disputes clause of this contract, that may arise as the result of the Government removing or ignoring authorized markings on data delivered under this contract.

(f) Omitted or incorrect markings.

(1) Data delivered to the Government without any restrictive markings shall be deemed to have been furnished with unlimited rights. The Government is not liable for the disclosure, use, or reproduction of such data.

(2) If the unmarked data has not been disclosed without restriction outside the Government, the Contractor may request, within 6 months (or a longer time approved by the Contracting Officer in writing for good cause shown) after delivery of the data, permission to have authorized notices placed on the data at the Contractor's expense. The Contracting Officer may agree to do so if the Contractor—

(i) Identifies the data to which the omitted notice is to be applied;

(ii) Demonstrates that the omission of the notice was inadvertent;

(iii) Establishes that the proposed notice is authorized; and

(iv) Acknowledges that the Government has no liability for the disclosure, use, or reproduction of any data made prior to the addition of the notice or resulting from the omission of the notice.

(3) If data has been marked with an incorrect notice, the Contracting Officer may—

(i) Permit correction of the notice at the Contractor's expense if the Contractor identifies the data and demonstrates that the correct notice is authorized; or

(ii) Correct any incorrect notices.

(g) Protection of limited rights data and restricted computer software.

(1) The Contractor may withhold from delivery qualifying limited rights data or restricted computer software that are not data identified in paragraphs (b)(1)(i), (ii), and (iii) of this clause. As a condition to this withholding, the Contractor shall—

(i) Identify the data being withheld; and

(ii) Furnish form, fit, and function data instead.

(2) Limited rights data that are formatted as a computer database for delivery to the Government shall be treated as limited rights data and not restricted computer software.

(3) [Reserved]

(h) *Subcontracting.* The Contractor shall obtain from its subcontractors all data and rights therein necessary to fulfill the Contractor's obligations to the Government under this contract. If a subcontractor refuses to accept terms affording the Government those rights,

the Contractor shall promptly notify the Contracting Officer of the refusal and shall not proceed with the subcontract award without authorization in writing from the Contracting Officer.

(i) *Relationship to patents or other rights.* Nothing contained in this clause shall imply a license to the Government under any patent or be construed as affecting the scope of any license or other right otherwise granted to the Government.

I.6 52.232-22 Limitation of Funds (Apr 1984)

(a) The parties estimate that performance of this contract will not cost the Government more than (1) the estimated cost specified in the Schedule or, (2) if this is a cost-sharing contract, the Government's share of the estimated cost specified in the Schedule. The Contractor agrees to use its best efforts to perform the work specified in the Schedule and all obligations under this contract within the estimated cost, which, if this is a cost-sharing contract, includes both the Government's and the Contractor's share of the cost.

(b) The Schedule specifies the amount presently available for payment by the Government and allotted to this contract, the items covered, the Government's share of the cost if this is a cost-sharing contract, and the period of performance it is estimated the allotted amount will cover. The parties contemplate that the Government will allot additional funds incrementally to the contract up to the full estimated cost to the Government specified in the Schedule, exclusive of any fee. The Contractor agrees to perform, or have performed, work on the contract up to the point at which the total amount paid and payable by the Government under the contract approximates but does not exceed the total amount actually allotted by the Government to the contract.

(c) The Contractor shall notify the Contracting Officer in writing whenever it has reason to believe that the costs it expects to incur under this contract in the next 60 days, when added to all costs previously incurred, will exceed 75 percent of (1) the total amount so far allotted to the contract by the Government or, (2) if this is a cost-sharing contract, the amount then allotted to the contract by the Government plus the Contractor's corresponding share. The notice shall state the estimated amount of additional funds required to continue performance for the period specified in the Schedule.

(d) Sixty days before the end of the period specified in the Schedule, the Contractor shall notify the Contracting Officer in writing of the estimated amount of additional funds, if any, required to continue timely performance under the contract or for any further period specified in the Schedule or otherwise agreed upon, and when the funds will be required.

(e) If, after notification, additional funds are not allotted by the end of the period specified in the Schedule or another agreed-upon date, upon the Contractor's written request the Contracting Officer will terminate this contract on that date in accordance

with the provisions of the Termination clause of this contract. If the Contractor estimates that the funds available will allow it to continue to discharge its obligations beyond that date, it may specify a later date in its request, and the Contracting Officer may terminate this contract on that later date.

(f) Except as required by other provisions of this contract, specifically citing and stated to be an exception to this clause—

(1) The Government is not obligated to reimburse the Contractor for costs incurred in excess of the total amount allotted by the Government to this contract; and

(2) The Contractor is not obligated to continue performance under this contract (including actions under the Termination clause of this contract) or otherwise incur costs in excess of—

(i) The amount then allotted to the contract by the Government or;

(ii) If this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, until the Contracting Officer notifies the Contractor in writing that the amount allotted by the Government has been increased and specifies an increased amount, which shall then constitute the total amount allotted by the Government to this contract.

(g) The estimated cost shall be increased to the extent that (1) the amount allotted by the Government or, (2) if this is a cost-sharing contract, the amount then allotted by the Government to the contract plus the Contractor's corresponding share, exceeds the estimated cost specified in the Schedule. If this is a cost-sharing contract, the increase shall be allocated in accordance with the formula specified in the Schedule.

(h) No notice, communication, or representation in any form other than that specified in paragraph (f)(2) of this clause, or from any person other than the Contracting Officer, shall affect the amount allotted by the Government to this contract. In the absence of the specified notice, the Government is not obligated to reimburse the Contractor for any costs in excess of the total amount allotted by the Government to this contract, whether incurred during the course of the contract or as a result of termination.

(i) When and to the extent that the amount allotted by the Government to the contract is increased, any costs the Contractor incurs before the increase that are in excess of—

(1) The amount previously allotted by the Government or;

(2) If this is a cost-sharing contract, the amount previously allotted by the Government to the contract plus the Contractor's corresponding share, shall be allowable to the same extent as if incurred afterward, unless the Contracting Officer issues a termination or other notice and directs that the increase is solely to cover termination or other specified expenses.

(j) Change orders shall not be considered an authorization to exceed the amount allotted by the Government specified in the Schedule, unless they contain a statement increasing the amount allotted.

(k) Nothing in this clause shall affect the right of the Government to terminate this contract. If this contract is terminated, the Government and the Contractor shall negotiate an equitable distribution of all property produced or purchased under the contract, based upon the share of costs incurred by each.

(l) If the Government does not allot sufficient funds to allow completion of the work, the Contractor is entitled to a percentage of the fee specified in the Schedule equaling the percentage of completion of the work contemplated by this contract.

I.7 52.252-2 Clauses Incorporated by Reference (Feb 1998)

This contract incorporates one or more clauses by reference, with the same force and effect as if they were given in full text. Upon request, the Contracting Officer will make their full text available. Also, the full text of a clause may be accessed electronically at this/these address(es):

http://www.acquisition.gov/far/

http://farsite.hill.af.mil/farsite_alt.html

I.7 HSAR3052.204-70 Security Requirements For Unclassified Information Technology Resources (Jun 2006)

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

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

(1) Within 60 days after contract award, the contractor shall submit for approval its IT Security Plan, which shall be consistent with and further detail the approach contained in the Offeror's proposal. The plan, as approved by the Contracting Officer, shall be incorporated into the contract as a compliance document.

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

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

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

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

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

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

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

I.8 3052.204-71 Contractor Employee Access (Jun 2006)

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

(1) Protected Critical Infrastructure Information (PCII) as set out in the Critical Infrastructure Information Act of 2002 (Title II, Subtitle B, of the Homeland Security Act, Public Law 107-296, 196 Stat. 2135), as amended, the implementing regulations thereto (Title 6, Code of Federal Regulations, Part 29) as amended, the applicable PCII Procedures Manual, as amended, and any supplementary guidance officially

communicated by an authorized official of the Department of Homeland Security (including the PCII Program Manager or his/her designee);

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

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

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

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

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

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

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

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

I.9 3052.215-70 Key Personnel or Facilities (Dec 2003)

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

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

The Key Personnel or Facilities under this Contract:

1. Program Manager

2. Program Leads

I.10 3052.242-71 Dissemination of Contract Information (Dec 2003)

The Contractor shall not publish, permit to be published, or distribute for public consumption, any information, oral or written, concerning the results or conclusions made pursuant to the performance of this contract, without the prior written consent of the Contracting Officer. An electronic or printed copy of any material proposed to be published or distributed shall be submitted to the Contracting Officer.
(End of clause)

Section J: Attachments

Attachment 1: Letter to Offerors (removed)
Attachment 2: Past Performance Survey (removed)
Attachment 3: Earned Value Management Self Verification Form (removed)
Attachment 4: Schedule B with Labor Categories and Hours.

NOTE: SOME ATTACHMENTS DO NOT APPLY TO AWARD.

Attachment 4: Labor Categories and Hours

SCIENCE APPLICATIONS INTERNATIONAL CORPORATION
TECHNOLOGY SERVICES COMPANY - COMPANY 6

LEISS and SOA for DHS ICE OAQ
HSCETC-09-R-00026

Proposed Staffing Plan by Labor Category

	Labor Category	BASE PERIOD	1ST OPTION YEAR	2ND OPTION YEAR	3RD OPTION YEAR	4TH OPTION YEAR
Development	Administrative Specialists	60	240	240	240	240
	Administrative Specialists (Senior)	22	115	115	115	115
	Application Systems Analyst	0	1,920	1,440	1,440	1,200
	Applications Engineer (Intermediate)	480	1,280	3,200	3,200	3,200
	Applications Engineer (Senior)	1,260	11,040	12,640	12,640	11,280
	Business Case Analyst	180	1,760	2,880	2,880	2,720
	Business Case Specialist	240	240	240	240	240
	Configuration Management Specialist (Lead)	240	1,280	1,120	1,120	1,280
	Functional Analyst	14	3,917	7,757	7,757	2,477
	Functional Analyst (Senior)	1,200	14,880	18,240	18,240	16,440
	Information Engineer (Principal)	570	4,560	4,560	4,560	4,520
	Information Resource Management Analyst	90	960	960	960	960
	Information Technology Senior Consultant	36	288	288	288	288
	IT Security Specialist (Senior)	0	1,920	1,920	1,920	1,920
	Project Control Specialist	660	2,826	2,186	2,186	2,106
	Project Manager	480	1,920	1,920	1,920	1,752
	Quality Assurance Specialist	54	1,272	2,232	2,232	2,232
	Subject Matter Expert	0	1,920	1,920	1,920	1,920
	System Developer	480	960	960	960	960
	Systems Architect	480	1,920	1,920	1,920	1,800

	Technical Writer/Editor	254	1,275	1,515	1,515	1,515
	Test Engineer (Intermediate)	150	960	960	960	960
O&M	Applications Engineer (Intermediate)	120	1,440	1,680	1,440	1,440
	Applications Engineer (Senior)	240	240	240	240	240
	Business Case Analyst	480	2,880	2,880	2,880	2,880
	Configuration Management Specialist (Lead)	240	640	640	640	640
	Information Engineer (Principal)	240	3,840	3,360	3,360	3,360
	Quality Assurance Manager	240	960	1,920	1,920	1,920
	System Developer	0	0	480	480	480
	Systems Engineer (Senior)	0	0	640	640	640
	Technical Writer/Editor	240	960	960	960	960
	Test Engineer (Senior)	120	960	1,440	1,440	1,680
Transition	Administrative Specialist					30
	Applications Engineer (Intermediate)					360
	Applications Engineer (Senior)					160
	Functional Analyst					40
	Functional Analyst (Senior)					160
	Information Engineer (Principal)					120
	IT Security Specialist (Senior)					80
	Project Control Specialist					10
	Project Manager					160
	Subject Matter Expert					80
	Systems Architect					120
	Technical Writer/Editor					30

Total Development	6,950	57,453	69,213	69,213	60,115
Est. Total FTEs	14	30	36	36	31
Total Operations & Maintenance	2,640	10,560	13,200	13,200	14,320
Est. Total FTEs	6	6	7	7	7
Total PMO	0	0	0	0	1,078
Est. Total FTEs	0	0	0	0	1