Award SOW

TASK ORDER REQUIREMENTS PACKAGE

1.0 BACKGROUND

Immigration and Customs Enforcement (ICE) is the investigative arm of the Border and Transportation Security Directorate (BTS), the operational directorate within the Department of Homeland Security (DHS) tasked with securing the nation's borders and safeguarding its transportation infrastructure. The largest component within the DHS, BTS employs more than 100,000 men and women. ICE brings together more than 20,000 employees who focus on the enforcement of immigration and customs laws within the United States U.S., the protection of specified Federal buildings, and air and marine enforcement. By unifying previously fragmented investigative functions, ICE will deliver effective and comprehensive enforcement. ICE is led by an Assistant Secretary who reports directly to the Under Secretary for BTS.

The Office of Chief Information Officer (OCIO)

The Office of the Chief Information Officer (OCIO), formerly known as the Office of Information Resources Management (OIRM), recently re-aligned its structure and operating model to be more responsible to the constantly evolving DHS environment, be more customer focused, and more efficient in providing the highest quality IT support to ICE. The OCIO is responsible for cultivating and maintaining an organization that provides high quality and timely IT services and products that reinforce ICE's ability to effectively and efficiently meet it's mission[1]. OCIO is also responsible for the administration, operation, and management of a broad range of support systems for ICE and its customers.

ICE OCIO Mission is to establish a viable organization that supports the mission of DHS, that is sensitive to the needs of its personnel and is focus on delivering quality service to its customers.

[1] **ICE MISSION**
To prevent acts of terrorism by targeting the people, money, and materials that support terrorist and criminal activities.
U.S. Immigration and Customs Enforcement (ICE), the largest investigative arm of the Department of Homeland Security (DHS), is responsible for identifying and shutting down vulnerabilities in the nation's border, economic, transportation and infrastructure security.

ICE VISION
To be the nation's preeminent law enforcement agency, dedicated to detecting vulnerabilities and preventing violations that threaten national security. Established to combat the criminal and national security threats emergent in a post 9/11 environment, ICE combines a new investigative approach with new resources to provide unparalleled investigation, interdiction and security services to the public and our law enforcement partners in the federal and local sectors.

2.0 OBJECTIVES

The SMI Contractor shall provide enterprise-wide information technology program management and integration support to OCIO as well as support and assistance in strategic planning and the oversight and coordination initiatives.

3.0 SCOPE OF WORK

The Systems Management and Integration (SMI) Contractor shall provide direct support to the ICE Chief Information Officer (CIO) by executing processes and procedures, which facilitate the management and integration of ICE information technology systems and applications. Support shall also include program management and integration, oversight and coordination of automation initiatives and investment management. In addition, the Contractor shall be responsible for ICE OCIO level systems engineering and support. This support includes but is not limited to, Systems Development Life Cycle management; configuration management, data management, quality assurance, testing, and all services required supporting the management of the ICE technical architecture. The Contractor shall also support implementation and management of OCIO information technology resources security and privacy programs and processes.

CIO-Sp2i Task Areas within the overall scope of this statement of work include:

- CIO-SP2*i*-Task Area 1 — Chief Information Officer Support
- CIO-SP2*i* Task Area 4 — Integration Services
- CIO-SP2*i* Task Area 5 — Critical Infrastructure Protection & Information Assurance
- CIO-SP2*i* Task Area 7 — Enterprise Resource Planning

4.0 SPECIFICATIONS

4.1 Contract Level and Task Order Management

4.1.1 Contract Level Program Management

The Contractor shall provide the technical and functional activities at the contract level needed for program management of this TORP including productivity and management methods such as Quality Assurance, Configuration, Work Breakdown Structure, and Human Engineering at the contract level. The Contractor shall also provide centralized administrative, clerical, documentation and other related functions.

Performance of this support shall be included for all subtasks within this task order as Not Separately Priced (NSP) Items.

4.1.2 Task Order Management

4.1.2.1 ICE Task Manager

The ICE SMI Task Manager is responsible for the oversight of the SMI Task Order. These duties include assuring that project activities are accomplished within the general scope of the task order, insuring adequate funding is available for authorized work, resolving task order level management and programmatic issues, approving other direct cost expenditures, when authorized; and facilitating effective interaction and coordination between ICE Project Leads and the contractor.

The ICE Project Lead will set technical performance priorities, provide operational guidance and initiate all changes to the task order technical baselines for their assigned project. The contracting officer will designate the responsible ICE Task Manager and Project Leads in writing, after award of the task order.

4.1.2.2 Contractor Project Manager

While the ICE Task Manager will provide management oversight of the task, it is the responsibility of the Contractor to manage all corporate resources and supervise all Contractor staff in the performance of all work on this task. The Contractor shall assign a Project Manager who will manage the day-to-day activities of the Contractor's staff. The Contractor's Project Manager is the member of the Contractor's management team who has responsibility for the actual accomplishment of the TORP requirements for this task. The Contractor's Project Manager shall organize; direct, and coordinate planning and execution of all task order activities, and will review the work of subordinates, including subcontractors, to ensure that the schedule, standards, and reporting responsibilities are met. The Project Manager shall integrate the Contractor's management and technical activities across all of the SMI projects to ensure they are consistent. The Contractor's Project Manager shall ensure that all work on this task complies with the contract terms and conditions and shall work with senior corporate managers, the Systems Management and Integration Contractor and ICE Managers to resolve any task issues that might arise. The Contractor's Project Manager shall be the primary interface with the ICE SMI Task Manager or designee. Performance of this support shall be included for all (Project Name) CLINS as Not Separately Priced Items (NSP)

4.1.2.3 Contracting Officer's Technical Representative (COTR)

The COTR is responsible for day-to-day contract administration activity such as: approval of other direct cost expenditure requests, acceptance of deliverables, review and approval of invoices, monitoring cost and schedule performance, enforcing task order terms and conditions recommending task order change requests and other duties as specified by the Contracting Officer. Only the Contracting Officer can authorize work to be performed or make changes to the terms and conditions or scope of this task order.

4.1.3 DHS-ICE IT Information Technology Management Concept

The OCIO will employ the DHS-ICE – IT Engineering Systems Assurance Program and integration management concept to manage the mandatory interaction of various Contractors delivering IT services on OCIO contracts and task orders. The primary tool for managing this interaction is the OCIO Interface Coordination and Control Working Group (ICCWG) made up of ICE technical managers, the performing Contractors, and a System Management and Integration (SMI) Contractor.

The National Institute of Health CIO-SP2i Government Wide Acquisition Contract will function as the primary acquisition vehicle for OCIO IT service requirements. Contractors selected to fulfill requirements from the CIO-SP2i contract will be directed, along with existing OCIO Contractors, to participate in the working group.

4.1.3.1 Interface Coordination and Control Working Group (ICCWG)

The Contractor's Project Manager or his designee shall at as Coordinator for the OCIO ICCWG. The ICCWG function as a forum for interaction and information sharing between the Government and the various Contractors performing on the ICE information technology contracts. Roles and responsibilities are described in the ICCWG Charter at Appendix D.

4.2 SMI Project Overview

The Systems Management and Integration (SMI) Program consists of the following subtasks.

TORP Section	Projects
TASK A	SYSTEMS MANAGEMENT, AND INTEGRATION SUPPORT
TASK B	INFRASTRUCTURE ENGINEERING SUPPORT
TASK C	ADP OPERATIONS
TASK D	COMPUTER AND TELECOMMUNICATION SECURITY SUPPORT
TASK E	UNIX SYSTEMS SUPPORT & DATABASE ADMINISTRATION SUPPORT
TASK F	IT INFRASTRUCTURE MANAGEMENT SUPPORT
TASK G	TECHNICAL REQUIREMENTS (OPTIONAL TASK)
TASK H	DECISIONS SUPPORT SYSTEMS

TASK A – SYSTEMS MANAGEMENT, AND INTEGRATION (TORP SECTIONS 4.3 & 4.4)

The Department of Homeland Security (DHS) is working to make effective use of IT by developing and implementing information systems that improve access to information across the Department and other Federal, state and local law enforcement entities. The U.S. Immigration and Customs Enforcement (ICE), within DHS, take a proactive position to integrate and modernize its IT systems to ensure that associated infrastructure are accessible, maintainable, industrious and easily modernized to meet future IT objectives and support the sharing and integration of information within DHS, other federal agencies plus state and local law enforcement organizations. ICE has established a Technical Architecture Program (TAP) to oversee and coordinate all technical architecture efforts in the Office of Information Resources Management (OCIO) and to partner with the ICE Office of the Chief Information Officer (OCIO) in the definition and implementation of the technology portions of the ICE Enterprise Architecture.

4.3 Architecture Assurance

The Contractor shall support the Architecture Assurance function in developing a comprehensive program for providing overall technical guidance, system assurance, standards, and direction for the development of applications and integrated IT infrastructure services. The Contractor shall recommend and help develop processes and technical approaches to support Architecture Program planning and coordination. The Contractor shall assist in the development of processes and technical approaches to support the following activities:

4.3.1 System Assurance

Systems Assurance embraces a number of disciplines, which when implemented in concert promote systems that fully achieve functionality, performance, interoperability, certification, quality, scalability, compatibility, and maintainability requirements. This task addresses these objectives through:

4.3.1.1 Quality Assurance (QA) Program

The Contractor shall be responsible for implementing an Enterprise-wide QA program, managing and modifying the program as necessary to ensure conformance and process improvement(s).

4.3.1.2 QA Oversight

The Contractor shall be responsible for implementing the ICE Enterprise QA program, managing, and modifying the program as necessary to ensure conformance and process improvements.

4.3.1.3 QA Requirements and Management Support

The Contractor shall maintain a QA Program that includes management, technical reviews and audits to validate the quality of work performed by development team personnel. The Contractor

shall provide assistance to the Architecture Program in defining the QA standards for all products and services, and audit compliance of project in using the required standards, as requested by the Architecture Task Manager. The Contractor shall be responsible for the following:

- Conducting an analysis of QA processes, to include mapping of AQ accomplishments to process improvement initiatives and established QA databases;
- Performing QA audits projects, as requested by the ICE Systems Assurance Manager
- Maintaining the QA Portions of the Enterprise Systems Assurance Plan (ESAP)
- Generating QA-related routine and special reports required by this task;
- Serving as QA point of contact for ICE generated AQ questions or issues;
- Proposing and documenting process improvements in AQ and associated areas;
- Providing training in the ICE AQ process and QA standards.

4.3.1.4 QA Product/Services Support

The Contractor shall:

- Serve in an oversight role and support IT Project Managers in the planning phase of the mission-critical development and maintenance tasks to:

  Ensure appropriate QA standards are applied;
  Identify the types and frequencies of review processes required to meet those standards;
  Integrate the development and/or maintenance schedules with sufficient time to allow for compliance with the applicable development life cycle and IT oversight processes.

- Use a standard QA process and methodology across all development tasks. Track, monitor, and audit selected development projects identified by the ICE Task Manager to ensure the quality of configuration management;

- Conduct periodic audits/reviews of work products for tasks identified by the ICE Task Manager to verify compliance to Enterprise QA standards. Perform project audits and reviews to determine project compliance to the life cycle or other appropriate standards. The Contractor's reviews/audits shall cover at a minimum, content and quality of project plans and deliverables. Any AQ issues should be acted upon/reported in accordance with standard AQ procedures.
- Monitor projects and manage noncompliance issues to facilitate resolution of issues related to process deviations and standards; and provide written notification of such issues to the ICE TASK Manager to determine course of action;

- Work with ICE TASK Manager when selecting an appropriate risk assessment, tailoring plan, or work pattern, and assist in identifying and using the appropriate work breakdown structure applicable to all projects;

4.3.1.5 Configuration Management (CM)

The TAP CM provides central management and oversight in the development and implementation of an Enterprise-wide CM program. The Contractor shall ensure that superior and reliable products are delivered to the Government. The Contractor shall maintain an ICE Electronic Library for the management of application components, and shall institute a standard and accessible change control process for all applications. CM activities include:

- Guiding and administering an ICE Enterprise-wide CM program applicable to all projects;

- Maintaining the CM portions of the ESAP;
- Providing configuration identification for software, hardware, and documentation;
- Initiating, controlling, tracking, and auditing changes, deviations, and waivers;
- Conducting configuration audits and reviews;
- Administering enterprise-wide use of PVCS Tracker and version Manager Software CM tools and ensure ICE investments and software assets are maintained;
- Managing and administering the Migration Request Tracking Systems (MRTS);
- Analyzing and evaluating CM software tools;
- Researching products and technical specifications;
- Maintaining and operating the ICE Electronic Library, which is a central library of documents and software.

4.3.1.6 Enterprise Lifecycle Management

The Enterprise Life Cycle Management functional component of the TAP establishes key architecture processes to support the ICE Technical Architecture. The Contractor shall ensure that an appropriate and flexible process is prescribed, maintained and disseminated to all stakeholders. This includes the following processes:

- Systems Development Life Cycle (SDLC) – provides a structured framework for managing system development and infrastructure projects and ensures that end-state systems and projects meet user requirements and support ICE strategic goals and objectives
- Requirements Services – enables ICE OCIO to establish, track, maintain, control and validate the functional and operational requirements for all ICE Systems in a disciplined and structured manner throughout the life cycle.

- QA-monitors projects and systems throughout the lifecycle to verify compliance with Technical Architecture standards
- CM-governs the integrity, control, and traceability of system products throughout the life cycle phases
- Architecture Test & Evaluation – ensures that software delivered to ICE meets functional, security, and performance requirements and is in compliance with the ICE Infrastructure
- IT Change Request – controls changes to the ICE Standards Profile.

These processes are documented in the SDLC, ESAP, Architecture Test & Evaluation Plan, and the Technical Architecture Guidebook.

4.3.2 Assessment and Compliance

Assessment and Compliance is charged with maintaining compatibility of systems in concert with the ICE Technical Reference Model (TRM), both as-is and target. The Design Phase of the SDLC serves as the most decisive point to evaluate system compliance with the target environment.

4.3.2.1 Design Review

Toward an objective of maintaining a viable technical architecture within ICE, the Contractor shall support both formal and informal reviews of all IT initiatives throughout the system lifecycle.

4.3.2.2 Requirements Management

The Contractor shall provide management support for Requirements processes, procedures, documentation, and tracking tools for all phases of the life cycle process.

4.3.2.3 Support to the Requirements Management Program

The Contractor shall provide support in establishing and maintaining a standard framework for the collection, storage, validation, and management of automated system requirements and in developing tracking mechanisms, documentation, tool sets, and business processes to improve requirements management practices. The Contractor shall provide support, as requested by the ICE Task Manager, in the review, assignment, justification, and tracking of requirements management documentation, including those generated by system developers, review boards, and user groups. The Contractor shall review and recommend revisions to ICE requirements management policies, processes, and procedures as requested by the ICE Task Manager. The Contractor shall be responsible for maintaining the Requirement Management portion of the Enterprise Systems Assurance Plan (ESAP). The Contractor shall also provide support in developing, coordinating, and implementing a program that ensures that requirements are integrated into project system initiatives. The program shall allow requirements traceability

matrices to be used to validate the design components; user participation in the development of system requirements; and the conduct of system readiness processes and evaluation. The Contractor shall revise the ICE Requirements Management Process Guide, as requested to reflect changes in the ICE Requirement management process and procedures.

The Contractor shall support ICE in establishing and maintaining a standard process for identifying, tracking, and resolving issues related to the IT project requirements. The Contractor shall provide training and briefings in the ICE requirements. The Contractor shall provide training and briefings in the ICE requirements management process, industry best practices in the field of IT requirements management, and use of the ICE requirements management library, as requested by the ICE Task Manager. The Contractor shall prepare all training materials required to conduct the training sessions.

4.3.2.4 Maintain Requirements Management Library

The Contractor shall manage and track requirements and requirement modifications for all automated projects. The management of the requirements includes tracking initial requirements from generation at the User Group meetings, through any change processes, to final incorporation into deliverable product(s). Baseline requirements are to be managed to facilitate test plan generation; tracking and management of requirements also includes documenting requirements that are initially generated by the User Group, but are then later deleted from the development project. All requirements information is to be stored and managed in a system that provides traceability information on specific requirements. This activity will also involve creating the necessary linkage and traceability.

4.3.2.5 Contractor Project Liaison

The Contractor shall provide technical and coordination guidance to support development activities regarding the technical architecture supported by ICE. The Contractor's Project Liaison may make recommendations regarding the structure and content of documentation, interrelationships of applications, address TRM interoperability, security, or standards enforcement issues and activities.

4.3.3 Functional Test and Evaluation

The Contractor shall support the Architecture Test and Evaluation (T&E) process and ensure that software delivered to ICE meets functional requirements and is in compliance with SDLC Processes. The Contractor shall support Architecture T&E while serving as the Independent Testing Facility (ITF) for all ICE systems and is tasked specifically with providing system-level testing and evaluation activities, as well as assisting users with acceptance testing activities. The Contractor's test and evaluation activities shall validate that delivered software meets the documented functional and interface requirements. The Contractor shall review and validate formulated requirements to ensure standardized refinement and traceability of the requirements allocated to the system components. The Contractor shall ensure that requirements are tested

and verified at the level specified. The Contractor shall assist in reviewing the proposed design solutions, in tracing the refined requirements definitions, and closely participate with system/user groups and SDLC phase review activities. The Contractor shall use the provided requirements traceability matrix as an effective tool in preparing a detailed specification describing the physical solution.

4.3.3.1 System Acceptance Testing (SAT)

The Contractor shall provide SAT services to validate whether a system satisfies its acceptance criteria. The Contractor shall evaluate user requirements to establish appropriate test metrics to ensure user development needs are met while maintaining ICE architecture compliance.

4.3.3.2 User Acceptance Testing (UAT) Facilitation Support

User Acceptance Testing (UAT) involves actual system users testing the software to ensure it meets user operational needs. The Contractor shall support UAT facilitation activities to include identifying, tracking and reporting all defects and discrepancies; providing management with daily and weekly status reports, and compiling anUAT Test Analysis Summary report;

4.3.3.3 Systems Security Testing

The Contractor shall provide Systems Security Testing services to evaluate the compliance of an operational system's technical controls with security and data integrity guidelines. The Contractor shall ensure systems developed on behalf of the Government meet the systems security requirements established for the ICE architecture. The Contractor shall identify security deficiencies and recommend alternatives to meet security requirements.

4.4 Architecture Engineering

The Contractor shall provide architecture-engineering services to ensure that the ICE technical architecture adequately supports the system functional requirements and provides interoperability between and among systems. The Contractor shall ensure systems developed on behalf of the Government meet the technical architecture requirements established for the ICE and DHS computing environments. The Contractor shall identify deficiencies and recommend alternatives to meet established and future requirements.

4.4.1 Information Integration

The Contractor shall provide the support necessary to develop and maintain ICE interoperability solutions and to perform data modeling to specify appropriate application logical data models for enterprise systems and to assist in transformation of such models into the appropriate physical data models.

4.4.1.1 Interoperability

The Contractor shall provide technical architecture guidance in support of strategies for data exchange and improved information sharing among systems. The premise is that systems are enhanced architecturally as additional data or business transactions from external systems are known. The approach to data exchange is through a common information hub, in which information routing, rules and transformations are centrally managed and operated to minimize the number of system –to-system data exchanges.

4.4.1.2 Data Management Services

In support of the sharing of process resources during application development, the Contractor shall develop and maintain the ICE Process Model component of the ICE Data Model. The Contractor shall accomplish this task by capturing, analyzing, and incorporating the ICE Business Processes from the ICE Applications that have their data requirements already incorporated in the ICE Data Model. The Contractor shall facilitate the sharing of information and process resources in support of the application development planning. The Contractor shall maintain training materials and documentation on the use of the ICE Data Model. The materials shall explain how the ICE Data Model will support the business application planning process and the application development process. Additionally, these materials shall address the issue of how compliance between the application logical model and the ICE Data Model is determined. When finalized, enhancements to the ICE Data Model shall be made as necessary, using the provided Designer 2000 tool. The Contractor shall continuously participate in the analysis of changes of the above components and provide electronic information, where available to support recommended alignment of projects within ICE priorities, and determine gaps, overlaps and changes. The Contractor shall review the possibility of common schema development. The Contractor shall assist Performance Contractors in understanding the technical capability of the ICE Data Model and monitor the Performance Contractors use of the standard tables as defined by Contractor. The Contractor shall publish the production version of the ICE Data Model using government provided tools. The Contractor shall maintain the ICE Data Model for the duration of the task period. Specific activities include:

- Update the ICE Data Model
- Update the Ice Process Model
- Provide support in reviewing ICE Application Logical Model(s) for compliance with the ICE Data Model.
- Implement the ICE Standard Data Tables
- Develop ICE Standard Data Table documentation
- Maintain and provide application level support for implemented ICE Standard data tables.
- Publish the ICE Data Model, in both document and website format
- Publish the ICE Process Model in both document and website format
- Maintain the ICE Meta-Data Repository.

4.4.2 Technology Integration

The ICE enterprise integration concept is a technical architecture approach to link existing systems and to provide the groundwork for future enterprise-enabled applications. Consequently, the ICE Technology base consists of an ever-evolving set of standards and products. To meet the challenges imposed by this continual evolution and upgrade, the Contractor shall provide the necessary support to meet the ICE technology integration requirements. Specific support includes simulation and modeling, technology domain planning and tactical project support.

4.4.2.1 Simulation and Modeling

At any point in the ICE technology evolution and the continuing evolution of the IT base, there may be a wide variety of product offerings and standards that offer upgrade possibilities, but whose advantages over present standards, cost of implementing and maintaining and unintended consequences are not known in advance. Simulation and modeling offers ICE the means of evaluating some parameters before making a high-dollar commitment and impacting the current architecture. The Contractor shall provide the support necessary to meet ICE simulation and modeling requirements.

4.4.2.2 Domain Planning

The ICE technical architecture must be continually monitored and evaluated for its effectiveness and efficiency in the support of current and planned applications and the enterprise architectural ideal of providing current, accurate and complete information to the user, irrespective of the location or position of the use r and the information systems that might contain that information. Standards and products must be evaluated and their insertion, either as replacement standards or contained standards, must be planned to help bridge legacy applications into an updated infrastructure. The Contractor shall provide the support necessary to ensure effective and accurate technology domain planning.

4.4.2.3 Tactical Project Support

The ICE technical architecture organization represents the central knowledge pool with regard to proper use of the technology products and standards that comprise the enterprise architecture. Through continual liaison with all applications and infrastructure projects, as well as the vendors and related consultants, technical architecture functions as a "clearinghouse" for best practices, and provides project consultation and support in the optimal use of these technologies. The Contractor shall provide tactical project support as necessary to ensure ICE projects have the best available "how to" knowledge provided to them.

4.4.3 Technical Test and Evaluation

Technical Test and Evaluation (T&E) evaluates the stability, capacity, response time, and throughput of a system by providing end-to-end integrated performance and interoperability testing for ICE systems. Technical T&E services include the use of custom test scripts, test automation tools, software and technical environment defect analysis and resolution, and IT product evaluation. The Contractor shall assist in the development of processes and technical approaches to support the following activities.

4.4.3.1 Lab Administration

The Contractor shall set up test environments and administer test lab facilities to provide ongoing support of ICE lab infrastructures which support: Systems Acceptance Testing, System Security Testing, Interoperability Testing, Performance Testing, Simulation and Modeling, and Application Tuning on behalf of the Government.

4.4.3.2 Interoperability Testing

The Contractor shall provide Interoperability Testing Services to validate that two or more systems can operate effectively when connected together. Interoperability Testing assesses the compatibility and potential impact of new or updated systems upon existing systems through the validation of their operation and conformity to approved architecture standards. It may be conducted with both manual or automated test tools and procedures. The Contractor shall identify discrepancies and make recommendation regarding feasibility of use for tested systems.

4.4.3.3 Integrated Performance Testing

Integrated Performance Testing evaluates the stability of a system by providing end-to-end integrated testing that measures system capacity, response time, and throughput among other parameters. The Contractor shall implement and operate an Integrated Performance Testing process that follows a methodology to coordinate, plan, execute, and document the results of the required testing activities during the full lifecycle of the development projects. The Contractor shall ensure activities are coordinated with all stakeholders according to schedules and plans, while enduring testing activities are thoroughly documented in support of lifecycle development activities.

4.4.3.4 Application Tuning

The Contractor shall provide performance application tuning services to identify technical design and development issues causing known or potential performance, stability and reliability problems.

4.4.4 Technology and Standard Policy

Within the ICE Technical Architecture Program, the Policy and Standards component provides for the planning of an integrated enterprise infrastructure, defines an interoperable and open Technical Architecture, establishes and administers enterprise-wide IT standards, establishes key policies and processes that support the Technical Architecture, and formulates strategies for the current and future Technology environment for ICE. The Contractor shall support the activities of the Technology Policy and Standards function.

4.4.4.1 Technical Reference Model (TRM)

The Contractor shall produce, document and maintain the ICE TRM by structuring IT services and processes across the enterprise to support ICE business processes to support the Business, Data, and Application layers of the ICE EA and to serve as the foundation on which ICE applications are built.

4.4.4.2 Standards Profile and Standard Documentation

The Contractor shall document the Technical Architecture standards by way of a Standards Profile. In conjunction with the *Standards Profile, the Contractor shall also maintains* an extensive collection of detailed standards documentation published to help project teams plan, design and build systems and infrastructures that conform to the ICE architecture. The current standards include:

Requirements standards

Enterprise data naming and structure standards

Data modeling standards

Standard lookup tables

XML data schema standards

Oracle database standards

IDMS standards

Web standards

Versioning standards

Product release standards

Structured cabling system standards

Domain name system (DNS) standards

Local area network (LAN) standards

The Contractor shall maintain these and develop additional standards documents as directed by the ICE Task Manager.

4.4.4.3 Technology Patterns

In conjunction with the Technical Reference Model, ICE maintains runtime patterns that identify specific technology integration approaches for each of the architecture platforms within its environment. The Contractor shall recommend, document, maintain, and otherwise develop these architectural patterns for the current and target ICE environments.

4.4.4.4 Enterprise Architecture Liaison

The Contractor shall provide liaison support to the ICE Enterprise Architecture planning activity. As the liaison, the Contractor shall research, document and generally facilitate integration between technology and enterprise business process.

4.4.5 Application Integration and Infrastructure Services

The Contractor shall provide the support necessary to maintain, improve, and manage the ICE web hosting environment infrastructure, and support the activities associated with hosting web-based Internet and intranet applications and websites.

Deliverables:

Application Integration and Infrastructure Services	Weekly Status Reports	Weekly

4.4.5.1 Web Infrastructure Services

The Contractor shall be responsible for maintaining operational status for the following Web/Application environments:

- E-Gov (production, test & evaluation)
- Intranet/Application Cluster/Isolated Application Clusters (production, support, test and development environments)
- Internet (production, support, and development)
- Dallas, TX contingency environment

The Contractor shall provide ongoing administration, monitoring, and technical support for all project infrastructure.

The Contractor shall provide infrastructure and operational support for the production environment on a "24x7x365" basis. Off-hour support (outside 7 AM to 5 PM) may be via "on call" personnel. The Contractor shall respond to trouble calls within one (1) hour of notification, or as otherwise indicated in the Service Level Agreement (SLA) associated with the hosted application. Problems are resolved within 24 hours of notification of the problem, or as otherwise indicated in the application's SLA. The Contractor shall, at a minimum, provide an update of each problem to the SMI Task Manager within four (4) hours of problem detection.

The Contractor shall follow established security requirements for maintaining an environment that ensures certification and accreditation requirements are met.

The Contractor shall review and analyze all production logs on a daily basis. The Contractor shall back up volatile data on a daily basis.

The Contractor, in close consultation with the ICE Task Manager, shall resolve operational problems in a timely manner.

The Contractor shall maintain standardized processes for deployment and maintenance of infrastructure components.

The Contractor shall comply with practices stated in the Application Integration and Infrastructure Change Control Board Charter for configuration management within the hosting environment.

Deliverables:

4.4.5.1	Web Infrastructure Services	System Activity Analysis Reports	Daily
		Maintenance Log Reports	Daily
		System Change Requests	As applicable
		Updated documentation to reflect all changes to the configuration	As applicable
		Technology descriptions, recommendations and analyses.	As requested
		Completed Infrastructure Change	As applicable

4.4.5.2 Web Hosting Services

The Contractor shall design, configure, implement, and maintain an infrastructure to provide a standardized hosting environment for ICE's web-based applications.

4.4.5.3 Web Application Integration Services

The Contractor shall provide ongoing management, monitoring and technical hosting support for all web-based applications within the ICE infrastructure. The current environment consists of various VB, JAVA, ASP, DHTML, XML, and HTML software, along with various COTS packages.

The Contractor shall meet with project managers to discuss standards and guidelines and best practices for development and deployment of their web-based applications.

The Contractor shall retrieve new versions of application software from Version Manager and load new/upgraded web-based applications into the applicable hosting environment.

The Contractor shall provide applications support for the production environment on a "24x7x365" basis. The Contractor shall respond to trouble calls within one (1) hour of notification, or as otherwise indicated in the Service Level Agreement (SLA) associated with the hosted application. Problems are resolved within 24 hours of notification of the problem, or as otherwise indicated in the Service Level Agreement (SLA) associated with the hosted application.

Off-hour support may be via "on call" personnel.

The Contractor shall analyze all production logs on a daily basis to determine operational issues.

The Contractor, in close consultation with the ICE SMI Task Manager, shall resolve operational problems within 48 hours, unless otherwise directed by the ICE SMI Task Manager.

The Contractor shall perform code reviews to ensure hosted applications comply with coding standards outlined in the Standards and Guidelines for Web Services. The Contractor shall create Test Problem Reports within PVCS Tracker for issues identified in code reviews.

The Contractor shall perform Web Environment Response Evaluations to gauge hardware resource consumption for hosted applications.

Deliverables:

4.4.5.3	Web Application Integration Services	Operational Status Report	Weekly
		Problem Status Report (may be verbal)	As applicable
		Updated documentation	As applicable
		Formal Code Review	As needed
		Test Problem Reports	As needed
		Web Environment Response Evaluation Report	As needed

4.4.5.4 Documentation Maintenance

The Contractor shall update, maintain and otherwise develop SDLC documentation for all aspects of this project. The Contractor shall maintain compliance with the current ICE SDLC version as of the date of the deliverable.

The Contractor shall update the Standard and Guidelines for Web Services document to ensure it remains current with AI&I requirements, versions of software components, infrastructure components, and best practices.

The Contractor shall maintain a project schedule that encompasses all tasks related to the Application Integration and Infrastructure task. The schedule shall be available to all team members.

Deliverables:

4.4.5.4	Documentation Maintenance	All SDLC specified documentation – as determined necessary by the Government. Task Manager Updated Standards and Guidelines for Web Services document Project schedule	As applicable As applicable On-going

TASK B-INFRASTRUCTURE ENGINEERING SUPPORT (TORP SECTIONS 4.5 THRU 4.17)

Infrastructure Engineering

The Infrastructure Engineering Infrastructure Engineering provides for all data communications needs for the Department of Homeland Security (DHS) Bureau of Immigration and Customs Enforcement (ICE) enterprise, and other networks which are located in the Continental United States (CONUS), Alaska, Hawaii, International offices, territories, and trusts. Specifically, Infrastructure Engineering Infrastructure Engineering is responsible for:

- Network engineering to research, design, test, document, and deploy new network systems solutions and develop network systems policies and procedures.
- LAN/WAN design, installation, troubleshooting, and user support for ICE International offices.
- Data communications equipment staging, configuration, installation, tuning, and turnover to production control to the NOC.
- Circuit ordering and tracking, as well as data communications equipment logistics, acquisition.

- Assistance with mission applications planning, development, and performance testing to ensure efficient network bandwidth usage and best possible response time/throughput across LANs and WANs.

- Cable plant management, engineering, design, installation, logistics, implementation and maintenance.
- Network address management functions including Dynamic Host Control Program (DHCP) servers to dynamically provide IP addresses, as needed, Domain Name Service (DNS), and NT Domain.
- Management and technical support to ensure consistent, responsive infrastructure and application deployments, integration of mission-related application development and deployments, and consistency of requested platforms within the installed base.
- Infrastructure platform management, engineering, design, installation, logistics, implementation and upgrades
- Manage, operate, and maintain the IT Infrastructure Engineering Lab and establish a consolidated Network Performance Lab to simulate, test, and certify configurations prior to production deployment.
- Operate and maintain a secure ICE Staging Facility for the receipt, secure storage, and shipping of Infrastructure platform and communications equipment and components.
- International Office technical support in the areas of technology assessments, planning, design, development, tracking, acquisition, system administration, system engineering, implementing, network assessments and inventory control
- Voice engineering and management support for the design, installation, logistics, implementation and maintenance of PBX systems.
- Voice management support for all voice related services including but not limited to cell phones, pagers, and calling cards.

4.5 NETWORK ENGINEERING

The Contractor shall provide network engineering support to research, design, test, document, and deploy new data communications network systems, solutions, policies, and procedures, including:

- Continuous improvement in the integration of ATM, FDDI, Frame Relay, MPLS, ISDN, SONET, and Point-to-Point circuit topology, along with OSPF, EIGRP, RIP, and other routing strategies;
- Engineer, design, implement, as well as maintain on an as directed basis, firewalls that access entities outside the ICENet and other networks supported by ICE. Implementation will involve: 1) Request for connectivity from external agencies handled by ICE

Managers, 2) Establish type of connectivity and termination point, 3) Contact the external agency and understand the application that will be used to access the external from the network or vice versa, 4) Identify the protocols and the ports that need to be defined on the firewall and formulate a secure rule to parse the packets, 5) Identify the changes at the desktop to be effected to make the secure connection, 6) Establish the rule set and the necessary protocols with the General Services Passer definitions but do not enable it, 7) Establish static routes at the firewall for the external connection but do not enable it, 8) On the testing date, bring up all rules and GSP services for the connectivity and test with users and developers. Maintenance may involve: 1) Cleaning up log files an archive on a regular basis, 2) Running Raptor log file analyzer and generate access reports for examine the reports for any anomalies, 3) Getting updates from Axent Technologies and effect the upgrades to the system at regular intervals, 4) Backing up configurations on a regular basis, and 5) Actively assisting in trouble shooting external access.

- Engineer, design, implement, as well as maintain on an as directed basis, Domain Name Service on ICENet and other networks supported by ICE. This will involve: 1) Supporting ICE Enterprise NT rollout, 2) Maintaining ICE Sector and District level administration autonomy while providing interfaces to 2nd and 3rd level support via Headquarters, 3) Supporting ICE mobile users by providing authentication service from any account domain (pass-through authentication) and implementing roaming user profiles, 4) Providing a consistent, manageable name space with unique user IDs for all employees, 5) Providing NT domain based authentication access to local and centralized resources, 6) Minimizing WAN traffic by using local authentication and WINS for NetBIOS name resolution and optimizing placement and relationships of domain controllers, 7) Inter-operate with the current ICE Office Automation (OA) environment including Windows95 (or current operating system) running either the Microsoft Client or the Novell Client32 and the NetWare 4.11 NOS (or current NOS) 8) Being compatible with current and future DHS security standards, and 9) Supporting ICE and DHS resource naming and communications standards.

- Design, document, implement, and assign network addresses, server names, and directory services to assist system deployment, including (but not limited to) IP and IPX addresses, local or global NDS Tree assignment, and NT Domain assignment. The Contractor shall operate an activity that provides one-stop shopping, for ICE personnel and support Contractors, to request IP addresses, IPX addresses, and server names. This service must be constantly staffed, from 8am to 6pm Eastern Time, 5 days per week. The function must be on-call via pager or other mechanism until 8pm Eastern Time. The existing one-stop shopping function is currently available via telephone, FAX, or cc:Mail. The Contractor shall work with ICE Web programmers to also provide the service on the OCIO Intranet Web Page. The Contractor shall operate the QIP Database to maintain the IP address ranges. The Contractor shall operate and maintain the DHCP function including trouble resolution. The Contractor shall also monitor and analyze the operation of these existing DHCP facilities, recommend design changes as needed, and deploy approved design changes. Deployment of approved design changes encompasses the

acquisition of any necessary GFE hardware or software, testing the new configuration, shipping equipment and material to the field, and installation at field locations.

- Identify, record, determine causes, and resolve performance bottlenecks with technical industry expertise and supported by the use of protocol analyzers and other real-time system monitoring tools;
- Develop specifications and upgrade data communications hardware and software to apply latest, proven technology to keep the LANs/WANs using state-of-the-art technology. This will involve engineering design, configuration, and recommending the most qualified vendor to supply the hardware and/or software.
- Design, document, implement, and train support personnel to operate access interfaces to mainframe or remote hosts using TN3270 emulation via TCP/IP protocols or SNA/SDLC gateways;
- Document and disseminate "lessons learned" or best practice solutions via written, oral, or Web-based reports;
- Train other support personnel in the use and support of data communications systems, policies, and procedures.

4.6 LOGISTICS – INFRASTRUCTURE ENGINEERING

The Contractor shall coordinate a multitude of logistical and administrative activities, including coordinating Branch activities with other organizational entities, assisting with acquisition of equipment and materials, maintaining the circuit tracking database, and providing the Branch with scheduling and administrative support.

4.6.1 Coordination

The Contractor shall coordinate the various functions and activities of the Infrastructure Engineering Branch. Contacts will include the Department of Justice, Department of Homeland Security, U.S. Sprint, M.C.I, RBOCS, Local Telcos, Equipment Vendors, Users, G.S.A. and other government agencies.

4.6.2 Acquisition

The Contractor shall assist with and coordinate the acquisition of equipment and materials associated with the daily operation of the Infrastructure Engineering Branch. This includes conducting documentation searches, preparing equipment specifications, preparing order documentation, and tracking deliveries.

4.6.3 Data Entry

The Contractor shall gather, organize, enter, and maintain accurate and current data into the Circuit Tracking Data Base, various spreadsheets, and the Infrastructure Engineering Branch intranet home page.

4.6.4 Scheduling Support:

The Contractor shall participate in the scheduling of all activities associated with the day-to-day operation of the Infrastructure Engineering Branch. This includes, but is not limited to deployments, technical projects, meetings, conferences, and trips.

4.6.5 Administrative Support

The Contractor shall participate in and provide administrative support for the preparation of various policies, directives, procedures, and documentation associated with the day-to-day operation of the Infrastructure Engineering Branch.

4.7 NETWORK MONITORING, PERFORMANCE, AND APPLICATION SUPPORT

The Contractor shall implement an enterprise-wide network and infrastructure performance plan to assist mission applications planning, development, and performance testing to ensure efficient network bandwidth usage and best possible response time/throughput across local and wide area networks. Specifically, the Contractor shall:

- Configure, deploy and manage network probes and other devices used for gathering data on the 1000 node ICE network and other networks supported by ICE. With these devices the Contractor shall capture and analyze circuit utilization data, WAN traffic flow patterns, and application workflow data.
- Coordinate with application software developers and managers to identify and document future plans for applications development and deployment. Advise software developers on ways to optimize utilization of network resources. Participate in applications design and development to ensure efficient network bandwidth usage and best possible response time and throughput across the local and wide area networks.
- Design, implement, and operate test bed to simulate full range of communication line speeds, bandwidth availability, routing nodes, repeater nodes, and other communication parameters. Develop models that represent the network infrastructure and applications that use the Data Communication Branch infrastructure.
- Develop performance test plans, conduct performance testing of existing or new applications, document test results, and disseminate "lessons learned" information to all applications development teams.
- Develop an overall approach that incorporates the network design, circuit utilization information, and future application software plans to predict future requirements for

topology changes, architecture changes, and utilization of components designed to speed the delivery of network data.

- Discrete and analytical simulation of models using varying network capacities, topologies, throughput rates, and design options to identify cost-effective network strategies.
- Analyze new technologies that will speed delivery of network data and provide predictable performance against business requirements from an enterprise perspective. Apply/adapt emerging technologies while supporting legacy systems in the ICE enterprise and other networks supported by ICE, to include interoperability with sister entities of the Homeland Security alliance.
- Contractor must also provide guidance to the DCB on:
- Designing and implementing content delivery solutions (load balancing, content filtering, distributed caching).
- Web hosting technologies and associated programming languages (knowledge of Web objects and HTML/XML tagging essential).
- Profiling applications to be supported in the infrastructure and identifying response time vulnerabilities prior to deployment.
- Optimizing data delivery from an enterprise perspective.
- The technical and business cases, in detail, for any proposed solutions at multiple levels (end user to executive).
- Identifying and explaining metrics associated with application transaction performance in a dynamic enterprise environment.

4.8 VIDEO TELECONFERENCING (VTC) - DELETED

4.9 CIRCUIT ORDER ANALYSIS

ICE is billed, on a monthly basis, for all of its data communications circuits. Currently, the monthly CDROM invoice is in excess of 1 gigabytes. These circuits are provided by many circuit providers and billed through the Department of Justice. After years of installing, de-installing and moving hundreds of circuits, discrepancies begin to accumulate in the billing documents. These discrepancies need to be identified and resolved in order to maintain an accurate billing structure.

The Contractor shall assess the data communications network topology and identify the monthly circuit expenditures to determine best practice, most cost effective circuit provisioning design technology. The billing reconciliation system is a web-based system. Specifically, the Contractor shall import the Department of Justice circuit billing data files or other billing data files as appropriate into a readable format (e.g. Excel spreadsheet or Access table). The Contractor shall group the circuit cost entries by circuit type, bandwidth, geographical area,

and/or cost factors. The Contractor shall also assemble lists of all existing data circuits. The Contractor shall compare the billing against the actual installed circuit list to identify any discrepancies. The Contractor shall recommend technology options to reduce ICE circuit costs.

The Contractor shall provide for the development, operation and maintenance of the existing Server and Web based system, as well as the on-going enhancement and expansion of the OCIO Intranet facilities or other Intranet facilities as appropriate. These facilities support the Service-wide operation of the Systems Integration Division or other organizations as appropriate. The Contractor shall be responsible for the technical support in the areas of technology assessment, planning, design, development, acquisition, system administration, Web site operation & maintenance and user support.

4.9.1 Technology Assessment

The Contractor shall perform research and analysis work on new Web technologies. The Contractor shall identify new and emerging Web related technologies, evaluate the applicability of these technologies, provide evaluation reports and recommendations, and test new and promising products.

4.9.2 Planning

The Contractor shall establish plans for the on-going expansion and enhancement of the OCIO Web facilities based on changing requirements, priorities and new technologies.

4.9.3 Design

The Contractor shall prepare designs for the expansion and enhancement of the OCIO Web system based on approved plans. The designs shall be based on the utilization of standard Commercial-Off-The-Shelf (COTS) products such as HTML, DHTML, Active Page, JavaScript, VB script, and FrontPage.

4.9.4 Development

Develop Web interface Client/Server application through the ICE Intranet using COTS products such as HTML, DHTML, MS Visual Studio, MS SQL Server, VB/ActiveX, CGI, COM/DCOM technologies and other appropriate technologies. Conduct thorough pre-production testing and verification of new hardware and software designs.

4.9.5 Acquisition

The Contractor shall develop acquisition documentation based on the approved plans and site design criteria. The documentation shall contain detailed specifications for the COTS equipment and software to be acquired and specify the number of units of each item required. The Contractor shall acquire COTS equipment and software necessary to deploy, operate, and maintain the Web Site(s) within approved plans.

4.9.6 System Administration

The Contractor shall administer access to the Web page, coordinate the entry and removal of data, and provide for the back up and security of the data. The Contractor shall install, configure, maintain, and trouble shoot Web software such as MS NT Server 4.0, MS IIS 4.0, and FrontPage 98.

- Web Site Operation and Maintenance - The Contractor shall operate and maintain the hardware and software facilities, related to the Web system, in order to provided reliable availability 24 hours per day, 7 days per week. The Contractor shall develop standards and procedures related to the operation and access of the Web Site.
- User Support - The Contractor shall work with end-users and provide technical support to design and implement their portions of the home page. The Contractor shall work with end-users to design and set-up standards for users interface, templates, and home page development and authoring tools. The Contractor shall provide new technologies research, consulting and training services to test and evaluate emerging information technology and to help streamline Web home pages functions. The Contractor shall also provide remote assistance to ICE field personnel accessing the Web Servers supported by DCB.

4.10 QUALITY ASSURANCE

From the Infrastructure Engineering Branch perspective, quality assurance is any systematic process of checking to see whether the services we deliver to our customers are meeting their specified requirements. A quality assurance system will increase customer confidence and the organization credibility, it will improve work processes and efficiency, and enable our organization to better compete with others.

4.10.1 Quality Assurance Program – Infrastructure Engineering Branch

The Contractor shall develop a program that continues to adapt quality assurance (QA) approaches supporting the Infrastructure Engineering Branch through 1) long-term process centric support for the development of institutionalized QA programs; 2) short-term customer centric technical assistance in the full range of modern QA methodologies; 3) a program of operations research; and 4) providing technical leadership in the application of QA.

4.10.2 Customer Satisfaction – Infrastructure Engineering Branch

The Contractor shall collect, document, analyze , and interpret the data regarding customer satisfaction on Infrastructure Engineering Branch services from call logs, trouble ticket, post-work surveys, interviews, and site inspection visits. Providing root cause analysis on the specific customer wants and needs, identifying areas for performance improvement, and making corrective or preventive recommendations to establish a new quality assurance benchmark.

4.10.3 Quality Assurance in Network Life Cycle

The Contractor Shall lead DCB efforts in building best practices, processes, procedures, documentation, and reporting to achieve Quality Assurance throughout the Life Cycle of the network. This includes creating an environment where QA engineers and network engineers work side-by-side during all phases of the product development cycle and facilitating meetings to coordinate processes and procedures both internal to QA and cross-functionally.

4.10.4 Organizational Policy and Procedures

The Contractor shall cooperate with management personnel to formulate, establish and maintain organization policies, operating procedures, objectives and goals. The Contractor shall assist with the initiation, development, and implementation of action plans for improvement in all business process, practices and procedures.

4.10.5 Quality Assurance Reporting – Infrastructure Engineering

The Contractor shall monitor and evaluate, and prepare reports indicating the results of QA observations by program and/or service. The Contractor shall also monitor inbound call quality, ticket quality and order implementation quality for outside sources (DHS, DOJ, GSA, telephone companies, vendors).

4.10.6 Test Plan

The Contractor shall coordinate with other Data Communication Branch Groups, to develop a test plan with documentation including test procedures, test guidelines, test scenarios, and test matrices. This test planning must include both a normal performance test and a stress network test, to ensure the response times and services delivered by the network fall within acceptable time limits under both normal and peak conditions

- Other activities include:
- Maintenance of QA documentation including minutes of meetings, up-to-date matrix of specifications/QA activities, glossary of QA terms, results of QA monitoring, formal QA reports.
- Development of a problem tracking system used to control and document any problems found within any process. Problems will be prioritized according to criticality.
- Recommendation of any additional tools or processes that will increase productivity or quality.

4.11 PROJECT MANAGEMENT OVERSIGHT

Project Management Oversight is the general administration, planning, organization, control and oversight, on a day-to-day basis, of major telecommunications projects to ensure that they are completed by the DCB on time and under budget. This includes the monitoring of a project in order to determine if the project is on schedule, within authorized budget, proceeding in conformance with the approved plans and specifications, and is being implemented efficiently

and effectively. Throughout the life of this task, the Contractor shall provide project management oversight to ensure the successful and timely completion of all tasks and deliverables. Project management deliverables shall include monthly status reports and project management plans as described in the following sections.

4.11.1 Project Management – Infrastructure Engineering

The Contractor shall provide project management support on major Information Technology (IT) telecommunications projects from initiation through implementation. This support will include phases such as planning, analysis, budgeting, design, development, and implementation. The Contractor will establish project requirements, priorities and deadlines and coordinate resources (staff, equipment, vendors and consultants) across one or more projects. Manage budget for assigned project(s), monitor project progress and adjusts resources and priorities accordingly. Prepare and presents progress reports for management using project management tools such as Microsoft Project and Project Central. Contractor shall apply performance management concepts to analyze cost, schedule, and technical performance of work packages, and also ensure that all elements of the project conform to Quality Assurance requirements. The Contractor shall coordinate among and between the task leaders, the Project Manager, and Government Organizations to develop integrated project schedules across multiple teams working on telecommunications activities.

4.11.2 Project Management Plan

The Contractor shall provide detailed project management plans that the DCB will use to identify the budget/cost considerations, technical issues, work breakdown structures, and scheduled milestones and objectives in support of DHS/ICENet initiatives. This plan must be consistent with the general management approach used to manage major U.S. Government projects and must detail the risks, budget, schedule, and technical issues, and identify work tasks for each of the DCB groups, as well as groups and agencies outside DCB as appropriate. This plan will establish the technical, cost, and schedule baselines to which the DCB projects will be managed and to which the performance of the project will be measured. Major schedule milestones will be defined, along with the cost estimate of each major subsystem to support this schedule. This plan must also describe the project management control mechanisms, configuration and change management, reporting requirements, and contingency procedures. This plan will be relied on by the management hierarchy within the DCB and OCIO to track ongoing projects, and outline the responsibilities between the DHS, BTS, ICE, and the DCB and all their users.

4.11.3 Project Management Reporting / Progress Reports

The Contractor shall provide brief progress reports to DCB once each month during the period that work is performed. These reports shall be submitted in duplicate no later than the 15th of the following month. The Contractor shall immediately notify DCB management of any significant breakthroughs or problems. Progress Reports shall be in a standard format and shall include at a

minimum the following subjects in the order indicated, with appropriate explanation and discussion:

- Title of project
- Reporting period
- Progress of project during the reporting period
- Identification of problems
- Planned solutions
- 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 cost incurred in relation to budget and progress to date, and ability to complete project within contract budget

4.12 PROJECT MANAGERS – INFRASTRUCTURE ENGINEERING

The connectivity services that the Infrastructure Engineering Branch provides to their customer base encompass a number of diverse functions, including; engineering and design, voice and data circuit ordering, network address management, router deployment, performance monitoring, and cabling. These services must be delivered as a seamless set to provide reliable, timely, end-to-end connectivity on the ICE WAN and other ICE supported networks. The Contractor supporting DCB shall provide a knowledgeable, technical team of project managers to accomplish this objective.

4.12.1 Project Cooperation and Management

The Contractor shall cooperate with management personnel to formulate, establish and maintain organization policies, operating procedures, objectives and goals. The Contractor's Project Managers shall be responsible for managing large-scale multi-disciplinary projects within the DCB network infrastructure. Responsible for the management of all assigned projects from inception through implementation including understanding customer requirements, planning/analysis/design, coordination between multiple DCB groups, documentation and resolution of issues, communication with end-users, implementation of network services, and follow-up and confirmation of project completion. The positions will also be expected to collaborate with Headquarters officials and field resources, to serve as customer focal point for network requirements, to manage teams implementing new network infrastructure in the field, maintain detailed schedules and tasking for network projects, and work with other Project Managers to ensure overall program success.

4.12.2 Project Management Support

The Contractor shall provide design, development, deployment, problem identification and remediation, and on-going support of the ICE global wide area network and other ICE supported networks. Work as a member of a project management team that takes part in the design,

deployment, and support of a WAN connecting all sites. The Contractor shall work independently, with only general guidance, to make independent decisions concerning: network engineering design, problem identification, and, problem remediation. The Contractor shall respond to network administration, operations, and maintenance problems while off duty, on an on-call basis.

Job Duties include:

- Independently manage a large, complex project that includes numerous communications components
- Develop and maintain project plans
- Act as liaison between varied project teams and DCB management
- Evaluate alternative solutions to business problems and make recommendations about technical and process solutions
- Define user requirements and functional specifications
- Review the work of project team members for accuracy and comprehensiveness
- Prepare scoping estimates for enhancements
- Coordinate the prioritization of tasks
- Manage Actions Items / Task List
- Prepare weekly project status report and meeting agenda
- Proactively identify and resolve project issues, escalate when appropriate
- Responsibilities and tasks may include, but are not limited to:
- Design and Engineering planning
- IP address management
- Determine appropriate circuit capacities
- Coordinate implementation schedules
- Tracking circuit orders with Government and Contractor personnel
- Effect changes in routing tables to migrate sites to new OSPF areas.
- Provide design engineering and implementation support for the design and deployment of the ICE WAN and other ICE supported networks, and LANs located at all sites.
- Provide 2nd and 3rd tier support to the Network Operations Center (NOC) to identify and correct WAN hardware, software, and circuit problems.

4.13 INTERNATIONAL OFFICE SUPPORT

The Contractor shall provide International Office technical support in the areas of technology assessments, planning, design, development, tracking, acquisition, system administration, system engineering, implementation, network assessments and inventory control. The Contractor shall test International Office hardware and software products, stand-alone equipment, and software applications as needed. All activities under this subtask must ensure that software and hardware will perform correctly over the Diplomatic Telecommunications Services Program Office Network.

4.13.1 Technology Assessment:

In support of the International Offices, the Contractor shall perform research and analysis work on new networking technologies. The Contractor shall identify new and emerging network operating systems, as well as various International Office LAN and WAN peripherals. The Contractor shall evaluate these products and provide ICE DCB with evaluation reports and recommendations.

4.13.2 Planning:

The Contractor shall establish plans for the expansion, support and operations of the International network and support operations.

4.13.3 Design:

The Contractor shall prepare designs for the expansion and enhancements of the International network and support operations. The designs shall be based on the utilization and/or migration to standard Commercial-Off-The-Shelf (COTS) products such as, but not limited to, Microsoft Office 2000. Windows 2000, and Exchange.

4.13.4 Development:

The Contractor shall work with COTS products and develop solutions to enhance International Office LAN/WAN operations and support capabilities. Other development activities may include Wide Area Networking technologies.

4.13.5 Tracking:

The Contractor shall provide DCB with tracking of inventory as well as tracking of tasks.

4.13.6 Acquisition:

The Contractor shall support DCB with the administration and physical acquisition of products in support of International Offices.

4.13.7 International Office System Administration:

The Contractor shall support existing and future International Office LANs. International Office support duties shall include add, moves, changes, deletion of LAN peripherals, users and software, maintenance of hardware, software and Network Operating System (NOS), and installations of new International Office sites.

4.13.8 International Office System Engineering:

The Contractor shall design, implement, deploy and support the International Office LAN/WAN components. These components consist of file servers, NOS, printers, switches, routers,

encryptors, workstations, CD ROM tower as well as any new technologies. International Office duties shall also include development of life cycle strategies for International Office LAN and WAN components and Wide Area Network analysis TCP/IP.

4.13.9 Implementation:

The Contractor shall perform implementation of International Office LAN/WAN components in the United States as well as in international countries.

4.13.10 Documentation:

The Contractor shall create and provide "as-builts" for historical purposes. These "as-builts" will include design, site survey, inventory (equipment), cabling standard, and a copy of the implementation plan.

4.13.11 International Office Network Assessments:

The Contractor shall assess current International Office LAN/WAN implementations and provide ICE DCB with recommendations for improving performance of LAN/WAN functionality.

4.14 ELECTRONIC DEPLOYMENT

The Contractor shall provide resources to support ICE management with the deployment of LAN/WAN electronics, including but not limited to CSU/DSU(s), routers, switches, and encryptors.

4.14.1 Installation:

The Contractor shall perform turnkey installation of routers and switches to domestic and international locations. Installation of the routers, switches, and encryptors will be done in accordance to ICE policy and procedures and will be implemented per the design provided by ICE. Installation of these devices may or may not require travel. If travel is required, the Contactor shall inform the ICE Task Manager and COTR of the requirement and shall be required to coordinate travel with all parties involved. Once the installation has been completed, the Contractor shall be required to remain onsite for 12 hours after the installation until the Government has provide acceptance. If no travel is deemed necessary by ICE management, the Contractor shall perform the installation over the phone with field personnel. Contractor shall continue to monitor the components for 12hours after installation has been completed. After the 12-hour period the Contractor shall be required to complete all required documentation and turn over the installation to the Network Operation Center for production monitoring.

14.4.2 Standards:

The Contractor shall follow ICE and industry standards during the installation of components. The Contractor shall work with ICE management to develop and modify standards as needed.

14.4.3 Configuration:

The Contractor shall configure routers and switches per the ICE standards to include standard operating system. All equipment needs to be burned in for at least 24 hours prior to deployment. The Contractor shall work with ICE management to establish or modify procedures for configuring components.

14.4.4 Procurement:

The Contractor shall procure equipment as needed to perform the installation of routers and switches. All procurements must be pre-approved by ICE management. All procured equipment must be entered into the ICE inventory management system. Procurement of equipment on behalf of ICE will be done in accordance with the Federal Acquisition Regulations as applicable.

14.4.5 Logistics:

The Contractor shall ensure that personnel, materials, and electronics arrive onsite and immediately corrected any deficiencies. The Contractor shall assist in ensuring the proper delivery of all components and associated materials and supplies required to properly and fully implement each project in accordance with ICE-approved design, Infrastructure standards, project schedules, and task statements. The Contractor shall coordinate the installation with HQ, field personnel, telephone companies and other parties that may be involved with the installation of the switches and routers. Contractor shall also be responsible for ensuring all components are properly entered into the ICE property management systems.

4.14.6 Documentation:

The Contractor shall create and provide as-builts for historical purposes. These as-builts will include design, site survey, inventory (equipment), cabling standard, and a copy of the implementation plan.

4.14.7 Communications:

The Contractor shall be required to hold pre installation and post installation briefing with our customers; therefore, the Contractor must have demonstrated superior oral and written communication skills.

4.15 INVENTORY – INFRASTRUCTURE ENGINEERING BRANCH

The Contractor shall perform inventory of equipment and resources located at all ICE Infrastructure Engineering Branch sites. The Contractor shall be responsible for the updating of the Action Request System (ARS) and the ICE Automated Management System (AMIS). The Contractor shall provide yearly inventory reports of all equipment and work with other ICE departments to locate and identify missing equipment.

4.16 VOICE COMMUNICATIONS PROGRAM SUPPORT

The Contractor shall provide voice communications expertise to assist the USICE in the continued development of service-wide voice communications policies and procedures. The Contractor shall provide technical advice on voice communications, the characteristics of transmission facilities to include switching and switches and public and private networks. The Contractor shall create wiring plans and telecommunications layout drawings; assist in the development of requirements documentation for telecommunications hardware and services; and assist in the continued development of USICE voice communications policies and procedures.

4.16.1 Headquarters Voice Communications Support

The Contractor shall assist with the identification, ordering, and placement of voice communications equipment, lines, and features requirements for office expansions, relocations, system enhancement additions, etc., and assist staff through the necessary approvals and placements of orders. Work requirements shall include the management of databases for work performed, lines provided, calling cards provided, pagers provided, cell phones provided, billing rates, and so forth. The Contractor shall maintain and publish an electronic and camera-ready telephone directory that will be used to produce hard copies and electronic copies. The Contractor shall also maintain and publish the telephone directory in Hypertext Markup Language (HTML) format for use on the USICE intranet website. The Contractor shall work directly with users, service providers, and ordering officials to insure that all voice services and equipment charges are accurate and that corrections are made as discrepancies are identified. The Contractor shall maintain regional and HQ inventories on pagers, cell phones, calling cards, PBXs, switches and lines.

4.16.2 Administrative Centers Voice Communications Support

The Contractor shall provide operational management of voice communications services at USICE Administrative Centers. At the Administrative Centers, the Contractor shall design and manage telecommunications projects as needed for USICE facilities and organizations throughout the Eastern Region area of operations, including travel to those locations to conduct site surveys, participate in project meetings, monitor installations and address post-installation issues. The Contractor shall provide technical advice on telephony, regulatory initiatives and general telecommunications services that support USICE business applications. The Contractor shall provide specialized knowledge of voice communications circuitry, switching, transmissions facilities, and networks. The Contractor shall provide first level trouble diagnosis and maintenance. The Contractor shall install and test voice communications equipment at the USICE Administrative Centers. The Contractor shall maintain all private branch exchanges (PBXs) at the USICE Administrative Centers, i.e., Lucent G3si, Mitel 1/w/ s/w 200 PBX, and Nortel Meridian Mail PBX. The Contractor shall oversee vendor installations and repairs at the USICE Administrative Centers.

4.16.3 Voice Communications Engineering

The Contractor shall provide voice communications expertise to assist the USICE in the development of voice communications technologies and design. The Contractor shall provide direct support to the USICE Systems Integration Division's Infrastructure Engineering (DataComm) staff and shall work in cooperation with Infrastructure Engineering Contractors as directed by USICE Infrastructure Engineering management.

4.16.4 Design and Deployment of Voice Network Systems

The Contractor shall develop designs for new PBX or other designated voice communication systems at ICE sites designated by DataComm Branch management. At DataComm Branch management direction, the Contractor also shall develop plans to fully implement those plans approved and selected by DataComm management.

At DataComm Branch management direction, the Contractor shall deploy systems according to designs and plans approved by management. The Contractor shall perform these deployments in concert with the DataComm Deployment Section and, when directed, shall work with designated DataComm Contractors.

4.17 CABLE PLANT MANAGEMENT AND SERVICES

4.17.1 Project Coordination

The Contractor shall work jointly with the ICE to provide management support services for the installation and maintenance of cable plants throughout the ICE. The Contractor shall be required to manage multiple projects at once. The Contractor shall be required to interface, coordinate, and liaise with personnel at ICE Headquarters, ICE Regional offices, Systems Integration Division, Department of Justice, General Services Administration (GSA), Core of Engineers and civilian Contractors, architects, and engineers. The Contractor shall be required to gather requirements, establish schedules, chair and attend meetings, communicate and coordinate projects with various cable Contractors, track project costs, and interface with Data Communication Branch (DCB) customers. In addition, travel will be required for attending construction meetings, project kick off meetings and performing site surveys, and quality assurance checks. The Contractor shall assist with modifications to policies, procedures, and standards.

4.17.2 Cable Plant Management Support Activities

The Contractor shall be required to provide cable plant management support for the ICE from beginning to end and ensure all documentation has been completed in accordance with the ICE agreed to project plan.

4.17.3 Installation, Maintenance, Repair, and Site Survey Support

The Contractor is also responsible for providing engineering support for the design, development, implementation, maintenance and support for all ICE Cable Plants.

The Contractor shall be responsible for the oversight and completion of all cabling projects. The Contractor shall be responsible for identifying that all materials (including incidentals and exhaustibles) acquired meet the ICE Infrastructure Cable Plant Standards. If the Contractor determines that materials do not meet the specified standards, the Contractor shall be responsible for notifying the ICE Task Manager. Also, the Contractor shall be responsible for ensuring that all procured equipment, except consumables, is entered into the ICE asset management system. The Contractor will also procure this equipment/materials at or below subcontractor/vendor GSA schedule prices and provide one-year warranty on parts and labor.

The Contractor shall provide the ICE with integrated cable plant installation services. For this effort, the Contractor shall provide cable, cable plant electronics (per ICE approved design), station and patch cables, face plates and surface mounts, patch panels, racks and other miscellaneous hardware, materials and labor used for the installation of a cable plant. The infrastructure cable plant shall be implemented in accordance with the ICE Infrastructure Cable Plant Standards and will adhere to all Local, State and Federal codes, and regulation. The Contractor shall be required to obtain any and all permits required to perform the cable plant installation. The Contractor shall be required to perform standard non-structural modifications as needed, this may include, but not limited to, core drilling, punch-down block installation, installation of plywood and mounting of communication racks. The Contractor shall be required to mount, patch, label, and document the cable plant electronics unless otherwise directed by the ICE Task Manager. Additionally, the Contractor shall test, certify, and label the entire cable plant installation; and provide As-Built documentation per the ICE Infrastructure Cable Plant Standards.

The Contractor shall also be responsible for providing support for a rapid response cabling team (i.e., "SWAT team") for emergency installations as directed by the ICE Task Manager. For CONUS sites, rapid response is defined as less than a 24-hour response. Each instance of a rapid response will begin with written authorization from the ICE Contracting Officer or COTRto the Contractor and will be funded similarly to other cabling projects. Due to the nature of this requirement, the Contractor must coordinate with the ICE Task Manager to provide the required deliverables and documentation required for cabling projects within an appropriate time frame.

The Contractor shall notify the DHS ICE Task Manager of cabling installation issues that arise that will jeopardize completion of cabling projects. This starts with a written report with 16 business hours of the discovery of the issue(s) and then continues with the trouble-shooting and dispatching of resources to resolve (personnel, equipment, materials, etc.) the issue(s).

The Contractor shall provide support for the resolution of LAN related trouble tickets to the extent of assigning trouble tickets and coordinating the solution.

Upon completion of the cable plant installation, the Contractor shall complete a documentation package. The COTR will issue a written acceptance of each cable plant installation after receipt and acceptance of all deliverables.

4.17.4 Cable Plant Management Quality Control Activities

The Contractor shall develop a Quality Control (QC) plan for infrastructure cabling that will be implemented in the performance-based environment. This plan describes how the Contractor shall perform quality control activities during the design, implementation, and certification for infrastructure cabling. Specifically, the overall QC plan must consider the following:

- Define the QC activities, sampling methodology, procedures, document templates, checklists and resources (including personnel qualifications and certifications) for each phase of a cable project
- Provide technical parameters for cabling installations based upon or considering ICE Infrastructure Cable Plant Standards and international quality control standards

4.17.5 PLATFORM ENGINEERING

Identify all IT data processing requirements and determining the suitability of all hardware, Operating System and related COTS used by the Bureau to support the ICE mission.

4.17.5. 1 Platform Configuration

The Contractor shall establish and identify minimum requirements for all computer hardware; server hardware, communications devices, operating systems and desktop applications to be deployed within the ICE IT environment. Determine a uniform standard for all equipment and peripherals deployed across the ICE system based on interoperability and functionality.

4.17.5.1.1 Identify Applications Processing Requirements

The Contractor shall identify specific application related hardware, operating systems and software requirements required to support ICE mission critical applications. This includes evaluating systems Bios, operating system capability and any special configuration or driver requirements.

4.17.5.1.2 Determine Hardware Configuration

The Contractor shall insure that all hardware (communications devices and software, workstations, servers, printers etc.) will support existing software, network connectivity and that it is fully compatible with related peripherals and systems. Also verify that all required drivers and any third party software is available within the system.

4.17.5.1.3 Determine Software Configuration

The Contractor shall analyze and verify that Operating Systems and COTS can be configured to meet mission requirements without impact to existing systems and capable of being standardized in a controlled image release.

4.17.5.1.4 Establish Platform Configuration Standards

The Contractor shall assist ICE in establishing technical standards that will allow the agency to stay current with its equipment and to interface technically with other department components. The Contractor (Lab personnel) may be required to participate in active ICE technical working groups (i.e., Architecture, Windows) with or on behalf of IT Infrastructure Engineering; in this event, the Contractor shall report on any action items at working group meetings. The Contractor shall provide written findings pertaining to the establishment or revision of technical standards in a separate section of the Monthly Progress/Status Report.

4.17.5.1.5 Develop Acquisition Specifications

The Contractor shall provide written technical specifications for the standard hardware software configuration requirements, once approved by the Government task manager. These standards are to be used by acquisition branch for procurement.

4.17.5.2 IT Infrastructure Engineering Lab

The Contractor shall staff and maintain the IT Infrastructure Engineering Lab, currently located at 801 I Street, Washington, DC. The Lab supports the following primary functions:

4.17.5.2.1 Develop and Update Standard and Custom Image Configurations

The Contractor shall develop and update standard and custom image configurations for every new model computer that ICE purchases. The Contractor shall configure and test the standard image for projects with unique and specialized requirements. The Contractor shall develop and test special project images, as directed by the ICE Task Manager. The Contractor shall maintain an electronic library of all images currently in use, which will be accessible to ICE at all times. The Contractor shall submit for ICE approval a detailed overview and layout of customized images developed with unique and specialized requirements and changes to the standard Infrastructure base platform.

4.17.5.2.2 Test Hardware and Software Compatibility

The Contractor shall test equipment and verify components with the appropriate image before it is shipped to the field to insure its compatibility with all automated data processing (ADP) software, hardware, and peripherals utilized by the ICE. The Contractor shall provide ICE with written results of all tests and present the impacts to ICE image and identify required changes for

application images. The Contractor shall deliver written findings of all testing to ICE written in accordance with the latest version of ICE Systems Development Life Cycle (SDLC) procedures. These findings shall be included in a separate section of the Monthly Progress/Status Report and posted on the ICE Infrastructure Engineering Intranet website.

4.17.5.2.3 Evaluate and Test New Technologies

At the government's direction, the Contractor shall evaluate and test new technologies, including hardware and software, to allow for key technical architecture decisions to be made with full knowledge of how equipment integrates with the rest of the ICE information technology. The Contractor shall proactively identify and evaluate products and technologies and research and evaluate any special new technology required by a program. The Contractor shall document the results of tests and evaluations and recommendations regarding products and technologies in a separate section of the Monthly Progress/Status Report; in addition, a list of technologies and products under review, test results, and documented recommendations shall be maintained on the ICE Infrastructure Engineering website. The Contractor shall also conduct, as appropriate, on-going analyses of the IT environment (i.e., network operating systems and servers) either through a simulated or a production system; the results of these analyses shall be documented in a separate section of the Monthly Progress/Status Report.

4.17.5.3 Staging Facility

The Contractor shall staff and maintain a secure ICE Staging Facility, such as the one currently located in Landover, MD. The Staging Facility shall protect the equipment stored in the facility from theft and damage (e.g., with monitored video surveillance 24 hours/day, appropriate lighting, alarms, etc.). The Contractor shall conduct a cost/benefit analysis for review by the ICE Task Manager prior to moving to another location. Staging Facility activities shall be conducted in accordance with Standard Operating Procedures (SOPs). The Contractor shall update the SOPs, as required, with ICE approval.

4.17.5.3.1 Receipt of Equipment

The Contractor shall receive all equipment, ordered by customers of the Infrastructure Engineering Branch at the Staging Facility. The Contractor shall inspect all incoming items for signs of damage and prepare equipment for storage and document details pertaining to damage or shortages in equipment orders. The Contractor shall provide copies of all staging receiving reports to both the Information Technology Solutions Management Center (ITSMC) and the ICE Task Manager for certification for payment. The Contractor shall apply ICE property management stickers to all equipment upon arrival and enter required information into the current inventory database. The Contractor shall recommend process improvements for logging and tracking the receipt of equipment and incorporate recommendations that are approved by ICE.

4.17.5.3.2 Inventory of Equipment

The Contractor shall maintain an up-to-date and accurate inventory (with not less than a 98 percent accuracy rate) of all equipment received at the ICE Staging Facility. The Contractor shall enter the necessary data into the current inventory data base and provide weekly inventory reports to the Infrastructure Support Branch. The weekly inventory report shall include a list of equipment on back order. The Contractor shall coordinate with the Infrastructure Liaison to provide quality assurance and "real-time" inventory information. The Contractor shall provide written notification to the Infrastructure Engineering Branch on any issues/concerns regarding inventory control, as well as weekly inventory reports and Quarterly Certified Inventory and Audit Reports.

4.17.5.3.3 Storage of Equipment

The Contractor shall store ICE equipment at the ICE Staging Facility. The Contractor shall track storage charges by ICE Program name and pallet count on a monthly basis. The Contractor shall submit a damage or theft report to the Infrastructure Engineering Branch upon discovery of such an incident and complete the necessary Computer Incident Response Program (CIRP) documentation.

4.17.5.3.4 Installation of Image

Based on technical direction from ICE Infrastructure Engineering Branch Team, the Contractor shall install the appropriate image on workstations, configure office automation (OA) servers, perform quality assurance (QA), and document the configuration prior to shipment. The Contractor shall also coordinate the installation of application servers and provide peripherals as requested. The Contractor shall perform front-end encryption on notebooks/laptops going to the field from staging.

4.17.5.3.5 Shipment of Equipment

Following setup and imaging of equipment, the Contractor shall prepare equipment for shipment following authorization by the Infrastructure Engineering Task Manager. Proposed shipping rates for all equipment stored in the staging facility must be approved by ICE. The Contractor shall provide ICE with the approved current Shipping Rates Schedule and notify ICE 60 days prior to any proposed rate changes. Prior to shipment, the Contractor shall update current inventory database to reflect G-504 location codes. The Contractor shall send G-504 forms with the shipment to the receiving site, notifying the site of transfer of ownership. The Contractor shall follow-up with customers to ensure that all G-504s are closed out within 15 calendar days of shipment.

4.17.5.4 Deployment Lifecycle Support

The Contractor shall work with the ICE Task Manager and the customer to identify specific requirements for the project and prepare a cost estimate and project plan. The majority of deployments require the Contractor to replace or upgrade existing IT hardware and software; in addition, the Contractor shall deploy equipment to newly established sites. The Contractor shall perform the deployment activities in accordance with SOPs. The Contractor shall update the SOPs as required, with ICE approval.

4.17.5.4.1 Pre Deployment Assessment Support

The Contractor shall assist the ICE in pre-deployment planning. Pre-deployment activities shall be conducted in conjunction with the identified Infrastructure Engineering Liaison and include conducting pre-site survey assessments, i.e., making contact with the customers, accessing and reviewing all available site documents; identifying current and planned activities; developing a preliminary deployment plan and schedule; and coordinating all infrastructure activities prior to visiting the site.

4.17.5.4.2 Site Survey Support

The Contractor shall conduct a Site Survey using an established, standard site survey instrument that covers, but is not limited to, the facility, the network topology, hardware and software inventory, and user needs. The site surveys will be conducted on site; however, there may be occasions when the Contractor, in conjunction with the ICE Infrastructure Engineering Task Manager, will determine whether the survey can be conducted by telephone or by field personnel.

The Contractor shall coordinate all site visits with the ICE Infrastructure Engineering Liaison. All site visits must be pre-approved by the USICE Task Manager. If the Infrastructure Engineering Liaison is not participating in the site visit, then the Contractor shall coordinate the site visit with the ICE Site POC.

The Contractor shall assist in developing site-specific Deployment Plans that describe the LAN design and equipment requirements for the site, cable plant design, and proposed Bill of Materials (BOM).

For each site, the Contractor shall develop and submit to ICE a Comprehensive Site Survey Report and one or more Trip Reports.

4.17.5.4.3 Acquisition and Logistics Support

ICE will acquire and make available to the Contractor hardware and software needed for deployment through the appropriate acquisition process. The Contractor shall receive, inventory, configure, and test all hardware and software to be deployed. These activities shall be conducted

primarily at the Staging Facility, with some testing occurring within the Image Lab. Hardware and software shall be deployed from the staging facility to the deployment site. Special circumstances may require "just-in-time" deliveries and on-site staging.

The Contractor shall coordinate all acquisition and logistics activities with the ICE Infrastructure Engineering Liaison. The Contractor shall work with the ICE Infrastructure Engineering Liaison to review and order BOMs for hardware and software, if applicable. The Contractor shall ship the equipment from the staging facility to the site(s) or arrange for "just-in-time" delivery in accordance with the deployment schedule. The Contractor shall track purchase requests and shipments to the Staging Facility and provide delivery information on a weekly basis to the ICE Infrastructure Liaison in accordance with SOPs. The Contractor may be required to resolve issues relating to the purchase of equipment or, if necessary, to expedite shipment.

The Contractor shall maintain the Master Infrastructure Site List and, in conjunction with the ICE Infrastructure Engineering Liaison, shall work with the sites to resolve any issues pertaining to the shipment, receipt, or condition of equipment.

4.17.5.4.4 On-Site Installation

Contractor personnel shall travel to the sites designated for infrastructure deployment and shall install and configure the hardware and software in accordance with the ICE approved Deployment Plan and Schedule. The Contractor shall verify site readiness, as defined in SOPs, prior to traveling to any sites.

The Contractor shall perform the following activities while on site:

- **Receive Equipment shipped from the Staging Facility** — The Contractor shall arrive on site to receive the equipment shipped from the staging facility or elsewhere in the case of just-in-time deliveries. The Contractor shall unpack boxes and inspect the equipment for damage and prepare for installation. The Contractor shall immediately report any damage or shortage to the ICE Infrastructure Engineering Liaison.
- **Conduct On-Site Inventory** — The Contractor shall inventory shipped equipment and notify Staging and the Infrastructure Engineering Liaison of any discrepancies. The Deployment Team Lead shall ensure that the G-504 is signed and accepted in AMIS. The Contractor shall return the signed G-504 to ICE Headquarters.
- **Coordinate all Deployment-Related Activities** — The Contractor shall work in concert with the ICE Infrastructure Engineering Liaison, the Site POC, cabling contractor, and any other support contractors, to ensure that the equipment installation proceeds smoothly, on schedule, and that the ICE mission objectives are satisfied. The Contractor shall provide the ICE Infrastructure Engineering Liaison with daily status updates during the daily meeting and a written daily report. The Contractor shall identify any issues upon discovery.

- **Install and Test Equipment** — The Contractor shall bring the system up to its full operational state. The Contractor shall review and update Standard Test Plans. The installed system shall be tested in accordance with an identified Standard Test Plan. After conducting the tests, a Test Analysis Report for each site shall be prepared and delivered to ICE. The Contractor shall provide "As Built" documentation to ICE.
- **Prepare Equipment for Excessing** — The Contractor shall assist the site by consolidating, boxing, and inventorying equipment identified by the site POC that is to be excessed with a palletized inventory that identifies the equipment on each pallet.
- **Coordinate Trash Removal** — The Contractor shall coordinate with the site POCs for the removal of trash generated by the deployment.
- **Conduct Close-Out Briefing** — After the equipment has been installed and tested, the Contractor shall conduct a close-out brief that presents the activities, results, and lessons learned from the site installation. If no ICE Infrastructure Engineering Liaison is available, the Contractor shall coordinate with the ADP POC on site to coordinate and lead the meeting. The Contractor shall ensure that the Infrastructure Engineering Team Lead and ADP POC sign the test and acceptance documents.

4.17.5.4.5 Post-Installation Support

Once a site installation is complete, the Contractor shall provide post-installation support to the site personnel. The post-installation support shall last up to five working days depending on the size of the site following the acceptance of the installed system by the ICE site personnel. During this period, the Contractor shall provide technical guidance and assistance to site staff and system users. The Contractor shall provide a limited amount of system administration functions and training to keep the system functioning. In addition, the Contractor shall provide assistance to the site personnel to communicate, coordinate, and facilitate Infrastructure Deployment project activities on site.

The Contractor shall provide ad hoc support, as needed, to local site staff during periods of high intensity deployment activity, such as facility modifications, cable plant installation, and post-installation transition. In addition, the Contractor may be required to provide temporary or permanent (local) on-site system administration support at selected sites.

4.17.6 Interface with Other Contractors Supporting the Infrastructure Engineering Branch Task

In providing the services described herein, the Contractor shall work in conjunction with other service providers under contract to ICE as follows:

1. NOC operation is provided on a full time (24 by 7) basis under a separate task. The Contractor shall:

   - Provide WAN design for (or review existing design by) the other Contractor;
   - Receive trouble ticket assignments from the NOC Contractor, provide expert analysis to resolve problems, record resolution into the NOC's trouble ticket tracking system, and de-brief the NOC Contractors on troubleshooting outcomes;
   - Request NOC Contractors to conduct link monitoring, trouble ticket tracking, circuit status update from previous shifts, and current system performance parameters; and
   - At the request of ICE, train other user support Contractors in implementing particular network performance enhancement procedures or equipment;

2. Under a variety of contract vehicles, ICE obtains International Office LAN/WAN Support from Northrop Grumman, Siemens, and through the Department of State. The Contractor shall:

   - Provide LAN/WAN design for (or review existing design by) Department of State, other technical Contractors;
   - Receive trouble ticket assignments from the Department of State Contractors, provide expert analysis to resolve problems, record resolution into the NOC's trouble ticket tracking system, and de-brief NOC Contractors on troubleshooting outcomes;
   - Request Department of State Contractors to conduct link monitoring, trouble ticket tracking, circuit status update from previous shifts, and current system performance parameters; and
   - At the request of ICE, train user support Contractors in implementing particular network performance enhancement procedures or equipment.

3. A separate task is used for equipment storage, staging, and deployment. The Contractor shall:

   - Direct equipment shipping, inventory tracking from the storage-staging-deployment Contractor for advance preparation of site installs

4. The Contractor shall interact with manufacturer technical support personnel providing hardware/software maintenance services to ICE. The Contractor shall work with vendor's technical support personnel to perform technical analysis, trouble resolution, design review, reporting, and user training. These vendors shall include, but are not limited to, the following:

   - Cisco

- Nortel
- Hewlett-Packard
- IBM
- Siemens/Pyramid
- Remedy
- Oracle/SQL
- Network General

5. The shall interact with various Long Distance Carriers and Local Exchange Carriers as follows:

   - The Contractor shall issue trouble tickets to the Long Distance or Local Exchange Carriers, provide expert analysis to resolve problems, report problem resolution to the exchange carriers; and
   - The Contractor shall request exchange carriers to conduct link monitoring, trouble ticket tracking, circuit status update from previous shifts, and current system performance parameters.

TASK C – ADP OPERATIONS (TORP SECTION 4.18)

4.18 ADP OPERATIONS SUPPORT

The purpose of the Contractor is to provide Information Technology (IT) infrastructure services to the United States Immigration and Customs Enforcement (BICE) worldwide.

4.18.1 BACKGROUND

The ADP Operations Branch is responsible for providing a secure, effective and responsive computing environment for the development, implementation, and maintenance of mission-critical and decision-support information systems. The Branch provides computer operations, database management, and systems software services. The Branch also has a major role in providing mainframe and enterprise UNIX systems support.

USICE has an Interagency Agreement (IAA) with the Department of Justice (DOJ), Justice Management Division (JMD), Information Resources Management, Computer Services Staff (CSS) to provide large-scale computing services to process and store mission-critical and decision-making data. There are two (2) Justice Data Centers (JDCs); one is located in Dallas, Texas (JDC-Dallas) and the other is located in Rockville, MD (JDC-Washington). USICE uses both Justice Data Centers for computing services.

Mainframe and enterprise computing services provided by the JDCs support a wide range of application programs and systems designed to enforce and support the immigration laws and codes and related missions of the USICE. As such, USICE applications systems must be available 24 hours a day, 7 days a week to immigration officers (i.e., USICE Inspectors,

Examiners, Border Patrol Agents, etc.) who are interviewing aliens, screening potential terrorists, and facilitating entry of persons legally admissible as visitors, citizens and immigrants. These functions are typically performed with a sense of urgency and in a time-sensitive environment at more than 1400 locations both within the continental U.S. and at numerous overseas locations.

4.18.2 Objectives

The purpose of this Task Order is to maintain contractor support for the seamless sustainment of Headquarters ADP Operations Support functions. Support provided will include, but is not limited to:

- Computer operations support required to operate and monitor the USICE MVS peripheral equipment, minicomputers (including UNIX-based), and microcomputers, at the HQ Operations Center;
- Production control support to process USICE data;
- Storage management support to manage and control USICE data that is stored on various storage media;
- Contingency planning support to minimize the impact of a disaster;
- Capacity planning support to ensure availability of required computing resources
- Systems software support to manage and control operating systems and product software; and
- Database management support of the USICE database management systems.

4.18.3 Requirements

The Contractor shall provide all necessary supervision, management, technical, and administrative support to accomplish this task order.

4.18.3.1 Computer Operations Support

The Contractor shall provide computer operations support required to operate and monitor the USICE environment of MVS peripheral equipment, minicomputers (including UNIX-based), and microcomputers, at the HQ Operations Center located in the Chester Arthur Building at 425 I. St. NW. The Contractor shall be required to perform printing services, backup and archiving procedures, disaster recovery, and prevention procedures. The Contractor shall also provide ancillary support services such as supplies control and limited facility management. The Contractor shall provide staffing coverage 24 hours per day, 7 days per week. Mandatory staffing shall be one (1) person per shift, including weekends and holidays. This subtask requires knowledge of Multiple Virtual Storage (MVS) and/or UNIX operating systems. Knowledge of Microsoft operating systems and Novell is desirable.

4.18.3.2 Production Control Support

The Contractor shall provide production control support for USICE application systems that are operational at the JDCs, HQ Operations Center, and other decentralized locations. Production control support shall include, but is not limited to, job scheduling; job submission; job recovery/restart; problem identification, determination and notification; input preparation; input/output control; output distribution; and database and file backup and recovery. Also, the Contractor shall perform system and on-line monitoring, and provide periodic reports on system unavailability and processing exceptions. The Contractor shall provide staffing coverage 24-hours per day, 7 days per week. The Contractor shall provide one (1) Systems Analyst or equivalent skill level, to staff the HQ Operations Center at all times, including weekends and holidays. The Systems Analyst shall ensure effective and timely problem identification, take the necessary corrective actions, and escalate problems in accordance with the ADP Operations Branch Problem Reporting and Escalation Procedure. This subtask requires knowledge of MVS or UNIX operating system, Job Control Language (JCL), automated scheduling packages (i.e., CA-Scheduler), Time-Sharing Option (TSO), and MVS or UNIX utilities.

4.18.3.3 Magnetic Media Library Management and Control

The Contractor shall manage and control magnetic media located at the HQ Operations Center and JDCs. At the HQ Operations Center, the Contractor shall manage and control storage, withdrawal, and return of magnetic media; and maintain and control magnetic media at offsite storage. At the HQ Operations Center and JDCs, the Contractor shall respond to user requests to manage data sets resident on USICE tapes; operate and maintain an automated media library management system; and maintain and execute a magnetic media rehabilitation and disposal program. JDC personnel will physically handle the magnetic media at JDC's. This subtask requires knowledge of MVS or UNIX Tape Management System (TMS) and TSO.

4.18.3.4 Direct Access Storage Device (DASD) Management and Control

The Contractor shall manage and control USICE assigned DASDs at JDCs. The Contractor shall complete establishment of storage management procedures and rules and use automated storage managers such as IBM's Data Facility System Managed Storage (DFSMS) and Data Facility Hierarchical Storage Management (DFHSM) to manage and control disk space for all USICE storage media. The Contractor shall also respond to user requests for disk storage space; maintain the integrity of USICE datasets residing on DASDs; maintain files and database backup and recovery procedures; perform disaster/recovery support; and monitor DASD usage and take appropriate action to minimize waste and abuse. This subtask requires knowledge of principles of storage management, including procedures and rules, and operational use of DFSMS, DFHSM, ABR/FDR, TSO, and MVS utilities or UNIX storage management products and utilities.

4.18.3.5 Capacity Planning

The Contractor shall provide capacity planning for USICE data processing at JDCs. The Contractor shall gather and conduct an analysis of USICE plans, develop workload projections, and prepare reports. The Contractor shall monitor USICE system usage and prepare reports. The Contractor shall also provide JDC budget planning and monitor costs. This subtask requires knowledge of principles of ADP capacity planning, modeling software, and presentation software.

4.18.3.6 Contingency Planning

The Contractor shall continue development, updating, administration, testing, and maintenance of an USICE ADP Contingency Plan for USICE applications systems at the JDCs. The Contractor shall stay abreast of USICE and JDC plans and make adjustments to the ADP Contingency Plan. This subtask requires knowledge of principles of ADP contingency planning.

4.18.3.7 Documentation

The Contractor shall continue development, maintenance, updating, storage, and distribution of the following documentation:

a. Existing procedure manuals and related documentation concerning functions performed and services provided under this contract.

b. New procedures manuals and related documentation, as directed by the Government, to provide comprehensive documentation for functions/services provided under this contract. The Contractor shall identify and recommend for Government approval topics that require documentation.

c. Develop bulletins, newsletters, change notices, system outage notices, and other written documentation to inform users about operations and other matters pertaining to ADP operations and related support.

d. SDLC documentation updates.

4.18.3.8 Technical Support

The Contractor shall provide technical assistance to support operating systems, DBMSs, and commercial software applications. The Contractor shall analyze and resolve problems, provide documentation of procedures and standards for the use of system software, and provide expert consultation on related technical issues. The Contractor shall develop and maintain an on-line notification and information system capable of disseminating and tracking documentation and change notices. As required by the Government, the Contractor shall provide IT services that conform to the USICE Systems Development Life Cycle (SDLC). These services shall include, but not be limited to, requirements analysis, design and development, and test and acceptance to support ADP operations activities.

4.18.3.9 Management Support

The Contractor shall provide the necessary operational management, project control, and technical expertise to provide technical guidance and direction to staff personnel. Additionally, the Contractor shall provide senior level technical storage management expertise and supervision to support capacity planning for USIC data processing at JDCs.

TASK D-COMPUTER AND TELECOMMUNICATION SECURITY PROGRAM (TORP SECTIONS 4.19 THRU 4.26)

The Contractor is to provide ~~C&TS~~ Office of Information Security Systems (OISSM) with products and services that support the ICE and DHS initiatives and ensure compliance with the mandated information security requirements as established by FISMA, DHS, ICE and NIST, as well as other government agencies as indicted.

The primary goal is to achieve cost effective and efficient compliance with information security mandates and develop ~~C&TS~~ OISSM program performance metrics, based on the DHS CISO Program Elements, that can be used as supporting information that indicates compliance with the current Security Act and/or mandates. Performance metrics must also allow for the tracking of metrics down to the Major Systems/Applications and General Support Systems (GSS) that will include ICE major offices or Sites. In addition, it is important to maintain continuity of the security program as it supports agency requirements and programmatic plans throughout the Systems Development Life Cycle (SDLC) of each IT system.

The Contractor is to assist the ~~C&TS~~ OISSM program with ensuring an operationally effective yet secure automated environment for existing and future information systems and applications by providing a strong, proactive team of practitioners that:

1) Understands IT architecture, SDLC and related issues;
2) Understands relevant Federal laws, and DHS policies, and other as listed
3) Provide a strong IA Program management and integration capability to effective design, implement and maintain a robust, comprehensive, efficient and cost effective ~~C&TS~~ OISSM IA program.
4) Review, interpret, develop, and disseminate the necessary ICE ~~C&TS~~ OISSM policies and procedures that reflect the DHS CISO's eight program areas and account for the guidance found in Attachment A.
5) Assist ICE in the development of an effective security solutions that addresses significant differences in multiple operational environments; develop risk management processes that are proven through utilization, and flexible enough to be valid as IT and user requirements evolve;
6) Develop and maintain an effective risk management and Certification and Accreditation (C&A) program that meets the requirements of FISMA, other oversight authorities, and other guidance found in attachment A. This must account for ICE requirements to perform C&A on Major Systems/applications and GSS, that address DHS and ICE policies and the ICE mission and operational requirements;

7) Develop, implement and maintain, in coordination with DHS and the ICE IT Training Program, a comprehensive Information Security Training, Education and Awareness Program that provides all requisite role based training required to ensure an effective IA program is fully implemented within ICE;
8) Design, develop and coordinate, with DHS and ICE IT Operational Organizations, Architecture teams, and System Assurance teams, the implementation of an effective IT Security Architecture that meets and complies with the DHS security architecture and meets ICE Operational and Mission requirements and IT operational needs and meeting IA requirements as identified;
9) Design, develop, enhance, and operate and maintain an effective Security Operations Center, Computer Security Incident Response Center, and Digital Identity Management Center (DMIC) to ensure that ICE is effectively securing and monitoring the security posture of its IT infrastructure and taking appropriate actions when threats, vulnerabilities, and/or incidents are discovered/reported;
10) Develop and maintain, in coordination with System owners, IT development and operations personnel, users and other necessary parties, to ensure development and implementation of an ICE wide Continuity planning program for all of the ICE IT Infrastructure and systems;
11) Develop, implement and maintain, as part of the ~~C&TS~~ OISSM Program Office, a comprehensive National Security Systems (NSS) or Classified IT security Program that meets the Executive, Federal, Department of Defense (DoD), DHS, ICE, or other agency NSS technical, management and operational controls requirements for the processing of NSS data.

4.19 C&TS PROGRAM MANAGEMENT AND INTEGRATION SUPPORT

The Contractor shall assist ICE in identifying strategic directions for the ~~C&TS~~ OISSM Program; review and revise existing documentation (e.g., ~~C&TS~~ OISSM Program Strategic Plan; legacy INS ATLAS plan); and support development of documentation charting the course of the Program. The Contractor shall coordinate this support with:

- ICE Senior management for strategic direction, initiatives, and implementation;
- DHS CISO Staff to ensure compliance with their program vision;
- ICE Chief Information Officer (CIO) for identification of compliance with the ICE CIO Mission, Vision and strategic planning;
- Other federal, state, local government and commercial CISOs; and
- And others as identified by the ICE ISSM.

The Contractor shall:

- Develop, maintain, and coordinate the implementation of the:
- C&TS Strategic, Tactical and Business Plans;

- Comprehensive Budget planning, execution, and tracking to ensure compliance with Federal, DHS, ICE and ~~C&TS~~ OISSM budget preparation and execution requirements; and
- The Contractor shall have the ability to accurately track all costs incurred for any non-ICE work conducted under this tasking.

- Research and advise on best practices in IA organizational structure, staffing and other related resource issues and ~~C&TS~~ OISSM program implementation.
- Research and prepare, responses as to internal and external data calls as directed by the ISSM and/or the Task Manager.
- Further the development, implementation, and enhancement of the ~~C&TS~~ OISSM Program by participating in meetings and subject matter conferences and seminars as required to keep abreast of ICE, DHS, and federal issues and trends in the ~~C&TS~~ OISSM arena.
- Attend conferences and industry symposia, when directed by the ISSM or Task Manager, to ensure continuing knowledge and awareness of state-of-the-art and market industry information relating to IA products, services, processes, practices, and techniques.
- Provide interface, coordination, and liaison with ICE personnel, ICE Contractors, and external partners to work with them to gain an understanding of requirements and to facilitate the inclusion of security capabilities in the planning of projects or activities requiring IA services.
- Provide support for ICE participation in the DHS and ICE IT Infrastructure steering and working groups, as directed.
- Ensure that all programs and major projects have a current and accurate Plan of Action and Milestones (POA&M); Budget projected and execution plan and reports; and that these are kept accurate (no less than monthly) and any significant (more than a week schedule slippage or a 5% cost) deviations are immediately provided to the ISSM and/or Task Manager
- Ensure that Program and project plans and budgets are in line and tie to the overall ~~C&TS~~ OISSM strategic, tactical and business plans and related budgets
- Provide overall on-site administrative support to the ICE ~~C&TS~~ OISSM Program Office to ensure its effective day to day operations

4.20 SECURITY POLICY

The Contractor shall provide technical support for the identification, development, establishment and dissemination of ICE, DHS and other appropriate policies, standards, procedures, and guidelines. In this capacity, the Contractor shall review Federal, State, and Local guidance, as well as, commercial standards for their impact on the ICE computing and security architecture.

~~Attachment A contains a non-inclusive list of applicable guidance that should be used as a baseline for the development of any ICE IA policy or procedures.~~

The Contractor shall perform:

- Research and apply knowledge of ICE IT operating environment and operational mission requirements to prepare ICE IA policies and procedures, facilitate their acceptance by ICE senior management, assist with their distribution of these documents to the Information System Security Officers (ISSO) Assistant ISSOs (AISSO), Designated Accrediting or Approving Authority (DAA), Systems Development teams, IT operations personnel, end users, and ICE Management personnel;
- Research and apply knowledge of the ICE operating environment to prepare position papers on policy and standards issues as directed;
- Review and comment on DHS and ICE standards and documents for relevancy and consistency with current ~~C&TS~~ OISSM Program processes and practices;
- Research, analyze and convert existing, ~~C&TS~~ OISSM guidance documents and technical bulletins into ICE policy statements and operating procedures;
- Develop policy and/or guidance for integrating IA requirements into Windows, UNIX, Novell, IBM Mainframe, CA Top Secret, and other IT environments as directed;
- Develop policy and guidance for securing remote access and external connectivity to the ICENET wide area network;
- Develop policy and guidance for securing Wireless technologies;
- Develop policy and guidance on the use of Portable Electronic Devices (PEDs);
- Develop policy, guidance, procedures and position papers on other IT technologies as directed;
- Maintain a ~~C&TS~~ OISSM web page to promote ~~C&TS~~ OISSM Policy and other program areas of the DHS CISO eight program areas; and
- Assist in the Service-wide distribution of other IT-related policy and procedures as required.

4.21 COMPLIANCE AND OVERSIGHT

The Contractor shall provide a variety of support functions to develop, implement, operate and maintain a comprehensive compliance and oversight program to address Risk Management and mitigation, Certification and Accreditation (C&A); FISMA self assessments and reporting; Office of Inspector General (OIG) audits, ICE CIO or ~~C&TS~~ OISSM Internal reviews and audits, and any other internal or external oversight and/or compliance activities. They will also provide guidance and assistance to assist in ensuring that all aspects of a comprehensive IA program is effectively implemented throughout ICE Systems and sites.

4.21.1 Information Systems Security Officer (ISSO) Support

The Contractor shall perform the following activities:

- Maintain a cadre of dedicated security professionals with diverse IT backgrounds to provide support to the ICE ~~C&TS~~ OISSM program and its ISSOs;
- Provide dedicated IT Security Analyst for each of the following ICE program areas: ICE Office of Information Resources Management, Air Marines, Federal Air Marshall, Intelligence, Investigations, Federal Protective Service, International Affairs, Internal Affairs and other ICE program as directed;
- Provide a cadre of up to 10 Regional ISSOs, as directed and as funding permits, who will act as an extension of the ISSM and perform as the Central ~~C&TS~~ OISSM representative for all ~~C&TS~~ OISSM efforts, including NSS functions, within their respective regions. They will work out of their homes, when practical, and will be expected to be on travel status at least 50 % of their time. They will:
    1. Act on behalf of the ISSM;
    2. Coordinate all ~~C&TS~~ OISSM initiatives within their respective regions;
    3. Visit all sites within their regions at least quarterly and provide training, education, and assistance to the ISSOs.
    4. Provide DHS IG support and other oversight/audit support to other regions, as directed by the ISSM and/or Task Manager
    5. Plan and coordinate regional Information exchange, training, etc working groups as directed by the ISSM and/or Task Manager.
    6. Act as a focal point for any Security incident until, and if, the ICE or higher CSIRC team responds.
    7. Must have a strong understanding of computer forensics and its application; Certification in this field is a plus.
    8. Must have a Secret Clearance and be clearable up to SCI.
    9. Certified Information Systems Security Professional (CISSP) certification or equivalent IA related certifications is highly desired; other technical certifications are also highly valued.
- Develop, implement, and maintain a model for establishing and supporting ISSOs.
- Maintain an ISSO Support Center for centrally supporting the Regional, System and Site ISSOs in all aspects of establishing and maintaining a local implementation of the ~~C&TS~~ OISSM program for their respective Systems or sites. The ISSO Support Center must interoperate with the ICE Help Desk, Security Operations Center, and Computer Security Incident Response Center and provide after hours support.

- Establish a local implementation of the ~~C&TS~~ OISSM Program at ICE HQ; including all activities associated with the ~~C&TS~~ OISSM program requirements.
- Facilitate a working group of ICE HQ ISSOs.

4.21.2 Risk Management Support

The ICE employs a multitude of automated systems to fulfill day-to-day, mission critical, information gathering, processing, and dissemination requirements. Much of the information processed by these automated systems is highly sensitive. There is some NSS or classified data processing occurring. However, it is expected to increase at some phenomenal rates over the next few years. Therefore, it is vital that all ICE information only be made available to the appropriate, authorized, and authenticated parties.

To ensure the security of the ICE automated systems and the information they contain, the ~~C&TS~~ OISSM Program has identified risk management as a key element of their Service-wide security strategy. Risk management consists of the disciplines, methodologies, and tools used to determine and quantify the relative value of a system, identify potential threats to the system and their appropriate countermeasures, as well as determining the appropriate level of support (resources and costs).

The ICE requires support in managing and mitigating risks associated with information systems. The ~~C&TS~~ OISSM program is responsible for providing guidance and technical direction in support of risk management, certification and accreditation (C&A), and FISMA assessments and various oversight or audit performed by internal or external organizations. In support of these endeavors, the ~~C&TS~~ OISSM Support Team shall provide proficient staff, proficient with implementation and use of known risk management tools, processes and concepts and good familiarity with System Development Life Cycle (SDLC) processes and IT Investment Management (ITIM) and Federal IT budget processes as they impact the implementation of an effective ICE ~~C&TS~~ OISSM IA program.

The Contractor shall perform the following activities:

- Develop, implement, and maintain a C&A program that minimizes the C&A process and empowers lower level approval authorities but complies with DHS and higher authorities requirements.
- Develop an ICE Risk Management Plan and manage its execution;
- Research, test, procure and install, when directed, an automated Risk Management tool to assist in streamlining and improving ICE abilities to meet the C&A and FISMA processes and requirements. This must interface with the DHS tools of choice for Risk Management, C&A and FISMA activities and reporting
- Provide guidance and technical direction in support of C&A, FISMA and other oversight related activities.

- Develop a schedule, in conjunction with the necessary DAA, ISSO and other relevant parties, for conducting and maintaining C&A on each system or application.
- Facilitate with the appropriate DAA, ISSO, and other relevant parties, risk management activities for all ICE major systems/applications and General Support Systems (GSS). This is to include guidance and assistance, and when directed, to prepare acceptable C&A documentation to include: System Security Plans (SSP), Risk Assessments, Security Operating Procedures or Guides, Security Test and Evaluations (ST&E) Test Plans (Pre-Operational and Operational), ST&E Test Plan Results Reports, Contingency Plans (CP), CP Test Plans and Results, Inter-Agency Security Agreements (ISA) and Rules of Behavior.
- Prepare and submit Security Evaluation Reports (SERs) for the Certification Official review and approval and submission to the appropriate DAA for the accreditation decision.
- Coordinate with the SOC for the conduct vulnerability assessments of information technology systems and networks in operational environments.
- Conduct and/or ensure the execution of a vulnerability assessment of systems in lab and pre-production environments as part of the risk assessment and ST&E processes.
- Perform site/system Design reviews/ walk-through and provide risk management advise to ISSOs and systems development teams to ensure that IA technical, operational, and management controls/requirements are being designed into the systems.
- Participate in and ensure that IA is being addressed thoroughly through out the SDLC process
- Participate in Systems Assurance and Configuration Management processes to ensure that IA requirements are being addressed and complied with.
- Assist System and LAN Administrators to identify security vulnerabilities in system administration processes and implement corrective measures.

4.21.3 FISMA Reporting and Self Assessments

Federal law requires government agencies to test their IT security on a regular basis, and Congress plans regular hearings to follow-up on government agency compliance. Self-assessments provide a method for agency officials to determine the current status of their information security programs and, where necessary, establish a target for improvement. The Guide's framework shall establish the groundwork for standardizing on five levels of security status and provide criteria agencies could use to determine if the five levels are adequately implemented (See NIST SP800-26).

The Contractor shall perform the following activities:

- Develop a self-assessment guide that provides an extensive questionnaire containing specific control objectives and techniques against which a system or group of interconnected systems

can be tested and measured. The guide shall not establish new security requirements. The control objectives and techniques shall be abstracted from existing requirements found in statute, policy, and guidance on security. This guide will be in compliance with DHS requirements and support the input of the necessary data into DHS choice of Automated Tool for complying with FISMA reporting, self assessments and remediation tracking;

- Provide ISSOs, DAAs, and other relevant parties training on FISMA requirements and how to use the procedures, guides, templates, automated tools that may be available for meeting the FISMA requirements. This effort should be coordinated with the Information Security Training, Education and Awareness ~~C&TS~~ OISSM support team as defined in activity 2.4;
- The Contractor shall provide technical support in conducting self-assessments by the various ICE components on their respective systems. This includes identifying corrective action to weaknesses and vulnerabilities identified during the assessment.
- Coordinate the ICE initiative to ensure accurate and timely submissions are made by the ISSOs and that the ICE FISMA reporting requirements are meet in accordance with DHS and higher authority directions.
- Coordinate and ensure the establishment of user accounts for all ICE ISSOs on the DHS tool of choice for complying with FISMA self assessments and reporting requirements; ensure that the ISSOs, in coordination with the Information Security Training, Education and Awareness tasking as defined in activity 2.4

4.22 INFORMATION SECURITY TRAINING, EDUCATION, AND AWARENESS

The Contractor shall provide a variety of support functions to institutionalize awareness of the ~~C&TS~~ OISSM Program and IA requirements. Specifically, the Contractor shall assist with coordinating an Information Security Training, Education, and Awareness training program. This program shall be in compliance with and complement the DHS Information Security Training, Education, and Awareness program requirements.

The Contractor shall perform the following activities:

- Attend Project Management meetings to educate ICE program managers in ~~C&TS~~ OISSM program and IA training requirements for both SBU and NSS systems;
- Coordinate all activity relating to the development and execution of an annual ICE or DHS five full day Security Conference;
- Provide a Plan of Action and Milestones (POA&M) for developing and implementing role based training for DAAs, ISSOs, System and LAN administrators; Database Administrators; IT Project Managers; Supervisors and Managers; end users; and Senior Executives;
- Design and develop Storyboards for role based training for DAA, ISSOs, System and LAN administrators; Database Administrators; IT Project Managers; Supervisors and Managers; end users; and Senior Executives

- Develop and implement role based training that will be accessible via the ICE Virtual University or CD-ROM for DAA, ISSOs, System and LAN administrators; Database Administrators; IT Project Managers; Supervisors and Managers; end users; and Senior Executives;
- Design, develop and implement an internal training and certification program for ISSOs that will be accessible the ICE Virtual University or CD-ROM. This should be based on, and adapted to the ICE environment, a recognizable professional certification like CISSP, CISM or SANS ISSO certification.
- Develop and conduct at least one awareness briefing (one half hour or less) and one training course (to be housed in the ICE Virtual University and CD-Rom), not to exceed two hours, for DAAs. This awareness briefing and training will focus on providing them with the requisite skills and knowledge they need to efficiently perform their DAA responsibilities
- Design and maintain a variety of awareness tools (posters, pamphlets, give a ways and training briefings),
- Provide revisions to existing C&TS, and create new, awareness pamphlets and facilitate the distribution of such materials agency-wide.
- Develop and provide for ISSM dissemination, through email broadcasts, a series of Security awareness emails to be sent, at a minimum monthly to all ICE users;
- Develop and produce a monthly newsletter for dissemination to ISSOs, DAAs, and other personnel with interest in the ~~C&TS~~ OISSM program;
- Support the planning for an ICE IA awards program for recognizing key personnel and organizations and their efforts and successes with respect to implementing key elements of the ~~C&TS~~ OISSM Program and IA requirements;
- Develop a POA&M, Storyboard and scripts to produce a ~~C&TS~~ OISSM Awareness CD to be distributed to all ICE Managers and Supervisors to make them more aware of the ICE ~~C&TS~~ OISSM program and how they can help ICE maintain an effective IA program.
- Develop a POA&M, Storyboard and scripts to produce an ~~C&TS~~ OISSM Awareness CD to be distributed to all ICE Users to make them more aware of the ICE ~~C&TS~~ OISSM program and how they can help ICE maintain an effective IA program.
- Assist and/or conduct annual Computer Security Awareness Training (CSAT) for ICE employees and Contractors
- Plan, coordinate, and implement an ICE IA Awareness Day to be conducted in conjunction with the Worldwide Computer Security Awareness Day. This is to include all ICE locations worldwide.

- Establish communications and dialogue with ICE and DHS Training organizations and facilities to integrate ICE ~~C&TS~~ OISSM Program precepts into their respective curriculums as necessary.
- Research the feasibility of obtaining an organizational membership in organizations like Computer Security Institute (CSI), Information Systems Security Association (ISSA) and having memberships for all ICE ISSOs;

4.23 SECURITY ARCHITECTURE

The Contractor shall support the on-going design, development, and implementation of a comprehensive information security architecture that is in compliance with the DHS Information Security architecture and meets the ICE mission and operational requirements to protect both sensitive-but-unclassified and classified information in electronic form and the systems which process, store, and transmit the information to ensure integrity, confidentiality, and availability, authentication and non-repudiation.

The Contractor shall provide technical skills and leadership to sustain and protect the ICE Technical infrastructure. The activity includes the development and implementation of an enterprise-wide integrated strong security architecture, establishment; staffing and operations of an Enterprise Security Architecture lab; Security Engineers to assist the various IT Operations and Program Development Teams to ensure that IA is addressed during the SDLC, Systems Assurance, ICE IT architecture, Configuration Management, and IT operations processes and procedures.

The Contractor shall perform the following activities:

- Design, build, staff and maintain an Enterprise Integrated Strong Security Architecture (EISA) lab that can emulate the ICE infrastructure. The lab will be used to test all new security products prior to be recommended to the ICE and/or DHS IT architecture teams for use within the IT Infrastructure. This will include SOC, CSIRC, DMIC/PKI, Auditing, PICS, Remote access and other technologies and other ~~C&TS~~ OISSM functions that require a technological solution to meet the ~~C&TS~~ OISSM program objectives.
- Develop and maintain an ESIA lab product testing plan and schedule.
- Develop the necessary SDLC and C&A documentation in accordance with DHS and ICE policies and procedures for any security solutions that area approved for deployment and use in the ICE/DHS IT Infrastructure
- Ensure that all Security COTS products, prior to deployment in an operational environment have been tested by Systems Assurance, approved by the IT Architecture and included as part of the ICE/DHS Technical Reference Models or appropriate waivers and exemptions have been obtained.
- Produce Product specific analysis and testing results documents.

- Research, design, and document an ICE Security Architecture that is in compliance with DHS security architecture and meets the ICE mission and operational requirements.
- Develop, when directed, Operating Systems (OSs) Hardening Guides for OSs that are used within ICE. The Contractor should use, when available and feasible, existing resources such as NSA Hardening guides as a baseline and modify as necessary to fit in ICE environments. This effort must be coordinated with the ICE IT architecture, Image lab, Systems Assurance, Systems Development teams, etc.
- Research, evaluate, acquire (as directed) and implement (as directed) various automated security policy, vulnerability scanning, and intrusion detection and prevention tools.
- Establish a strategy for updating, deploying and maintaining ICENET protection tools.
- Research, design, document a strategy, and implement when directed, to improve the functionality and operations and maintenance of the Password Issuance and Control System (PICS); and
- Conduct an analysis of the existing ICE, Department of Justice (DOJ) and DHS Secure Remote access solutions that are currently being used by ICE personnel, and determine, based on ICE remote access requirements, recommend and engineer a single ICE solution that meets DHS and ICE security architecture and meet ICE Mission and operational requirements for fast, secure and reliable remote access.
- Assist, as directed, in the development of the Consolidation Tracking Repository System;
- Investigate and make configurations improvement recommendations on the ICE implementation of CA/Top Secret in the mainframe environment;
- Participate in the development and modification of ICE automated systems and applications to ensure effective integration of required security features.
- Develop an identification and authentication model/protocol/strategy (Single Sign on) for all ICE systems and applications.
- Research and enhance, when feasible, a robust virus prevention strategy for Service-wide implementation.

4.23.1 Auditing, Review and Consolidation of Audit Records

Research, plan, coordinate, acquire (when directed) and implement (when directed) a solution for effectively integrating audit capabilities into the Windows, UNIX, IBM mainframe and user workstations; The ~~C&TS~~ OISSM Task Order Support Team will support the development and fielding of a system user activity and auditing capability. Specific functions required by this activity include the following:

- Evaluate products required to perform auditing on ICE IT infrastructure components and provide appropriate recommendations for product selection
- Obtain products for evaluation within EISA lab and produce product evaluations reports;

- Design, implement, and monitor pilot implementations, in an ICE operational environment, of products recommended for use in the ICE security architecture
- Develop Standard Operating Procedures addressing the use of the selected products
- Provide appropriate training and documentation on the use on the selected products
- Develop an implementation schedule that will ensure distribution of auditing software to ICE Major Systems and GSSs;
- Coordinate with the SOC, the transfer of this capability as it is developed and ready to be made operational;
- Support the SOC, as required, in administering and maintaining event collectors, centralized data analysis, and management components;

4.23.2 Privacy and Public Key Infrastructure (PKI)

Under the Government Paperwork Elimination Act (GPEA), Pub. L. No. 105-277, executive agencies are required, by October 21, 2003, to provide "for the use and acceptance of electronic signatures, when practicable." Under the OMB Guidance, Procedures and Guidance on Implementing the Government Paperwork Elimination Act, the Department of Homeland Security is charged with developing, in consultation with federal agencies and OMB, practical guidance on legal considerations related to agency use of electronic filing and record keeping.

The explosive growth of the Internet has led to great concern about system and network security, including information confidentiality, integrity, and authenticity. PKI provides the overall framework and individual tools that allow organizations to satisfy one or more of the following objectives: use certifications to authenticate users; create secure communications channels; and sign content in a way that guarantees non-repudiation. PKI can also reduce overall security costs and increase interoperability within and between enterprise systems.

Because of the cost and complexity of implementing PKI, in the future, most enterprises will use multiple levels of assurance (e.g., low, medium, high) to ensure that the more complex and costly security solutions are applied to those individuals requiring high assurance capabilities.

To support this activity, the Contractor shall:

- Conduct an analysis of the nature of ICE systems and applications to determine the level of protection needed and the level of risk that can be tolerated. The Contractor should use the Risk Management, C&A and FISMA documentation to gather this information
- Define the roles to be played by the electronic signature and adopt the electronic signature technology or technologies that best serve those purposes.
- Benchmark PKI processes and procedures used by civilian, government, and other law enforcement agencies
- Develop a list of PKI alternatives that can be used by ICE.

- Support the operation of the PKI Lab or infrastructure, as a part of the EISA lab if feasible, at the Contractor's facility that can be flexibly configured to simulate the ICE IT infrastructure and used to test and demonstrate PKI components and capabilities.
- Acquire the hardware, software, and services required to implement a PKI Infrastructure within the EISA lab, as directed.
- Define requirements; develop designs, implement prototypes, and support pilots for PKI components.
- Conduct a market survey of available commercial off-the-shelf (COTS) products to identify products that best meet ICE and DHS requirements for PKI component.
- Evaluate PKI products and recommend the best products for use in prototyping, and document the process and results in a monthly product evaluation report.
- Integrate COTS products together, as appropriate, to implement PKI components. Where suitable products are not available, ICE may task the Contractor to develop the missing component.
- Implement a PKI prototype. Demonstrate prototype to both ICE and DHS representatives, modifying as necessary to obtain DHS acceptance.
- Coordinate and conduct the analysis and evaluation of the PKI/Cryptographic Services Infrastructure (CSI) component.
- Define requirements, develop the design, and implement a prototype for the Cryptographic Services Infrastructure component and also manage and conduct a CSI Pilot. CSI Pilot activities shall include:
- Provide installation guides, operation guides and training support for the pilot.
- Provide acquisition support to the ICE for the hardware, software, and services required for the pilot.
- Prepare the pilot evaluation report.
- Develop a transition and implementation plan, in coordination with the Digital Identity Management Center personnel that ensures compliance with the ICE and DHS security architecture and the ICE Mission and operational requirements.
- Develop training and standard operation procedures for the chosen alternative.
- Support the implementation of the PKI technology.

4.23.3 Smart Card Technology

Smart cards are widely acknowledged as one of the most secure and reliable forms of electronic identification. Smart cards have the unique ability to store large amounts of biometric and other data, carry out their own on-card functions, and interact intelligently with a smart card reader.

Secure ID systems that require the highest degree of security and privacy are increasingly implementing both smart card and biometric technology.

Biometric technologies, when used with a well-designed ID system, can provide the means to ensure that an individual presenting a secure ID credential has the absolute right to use that credential. Smart cards provide the secure, convenient and cost-effective ID technology that stores the enrolled biometric template and compares it to the "live" biometric template.

Using smart cards significantly enhances privacy in biometric ID systems. It secures personal information on the card, allowing the individual to control access to that information and removing the need for central database during identity verification

Smart cards can store digital certificates for secure transactions over the Internet, be a container for vital information, store a biometric for positive identification, and can be used to make purchases or exchange value.

The Contractor shall perform the following activities.

- Define the roles to be played by the Smart Card Technologies and adopt the technology or technologies that best serve those purposes.
- Benchmark Smart Card processes and procedures used by civilian, government, and other law enforcement agencies
- Develop a list of Smart Card alternatives that can be used by ICE.
- Provide recommendations for product selection based on the evaluation of the alternatives.
- Define requirements; develop designs, implement prototypes, and support pilots for PKI components.
- Develop an implementation plan that ensures compliance with DHS/ICE security architecture and ICE Mission and operational requirements.
- Develop training and standard operation procedures for the chosen alternative.
- Support the implementation of the technology.

4.23.4 Biometrics

Biometric technologies are emerging as a viable security solution on many fronts, including government, IT and the enterprise. Biometrics are automated methods of recognizing a person based on a physiological or behavioral characteristic. Among the features measured are; face, fingerprints, hand geometry, handwriting, iris, retinal, vein, and voice. Biometric technologies are becoming the foundation of an extensive array of highly secure identification and personal verification solutions. As the level of security breaches and transaction fraud increases, the need for highly secure identification and personal verification technologies is becoming apparent.

Biometric-based authentication applications include workstation, network, and domain access, single sign-on, application logon, data protection, remote access to resources, transaction

security and Web security. Utilized alone or integrated with other technologies such as smart cards, encryption keys and digital signatures, biometrics are set to pervade nearly all aspects of IT operations. Utilizing biometrics for personal authentication is becoming convenient and considerably more accurate than current methods (such as the utilization of passwords or PINs). This is because biometrics links the event to a particular individual (a password or token may be used by someone other than the authorized user), is convenient (nothing to carry or remember), accurate (it provides for positive authentication), can provide an audit trail and is becoming acceptable and inexpensive.

To support this effort, the Contractor shall:

- Benchmark biometric methods used by civilian, government, and other law enforcement agencies
- Develop a list of biometric alternatives that can be used by ICE.
- Provide recommendations for product selection based on the evaluation of the alternatives.
- Define requirements; develop designs, implement prototypes, and support pilots for Smart Card implementation.
- Develop training and standard operation procedures for the chosen alternative.
- Develop an implementation plan that ensures compliance with DHS security architecture and ICE Mission and operational requirements.
- Support the implementation of the technology.

4.23.5 Virtual Private Network (VPN) Technology

A virtual private network (VPN) is a private data network that makes use of the public telecommunication infrastructure, maintaining privacy through the use of a tunneling protocol and security procedures. A virtual private network can be contrasted with a system of owned or leased lines that can only be used by one company. The idea of the VPN is to give the company the same capabilities at much lower cost by using the shared public infrastructure rather than a private one. Phone companies have provided secure shared resources for voice messages. A virtual private network makes it possible to have the same secure sharing of public resources for data. Organizations today are looking at using a private virtual network for both extranets and wide-area Internets.

Using a virtual private network involves encrypting data before sending it through the public network and decrypting it at the receiving end. An additional level of security involves encrypting not only the data but also the originating and receiving of network addresses.

To support this activity, the Contractor shall:

- Provide recommendations regarding the design, procurement and deployment of a VPN.
- Develop Standard Operating Procedures addressing the use of a VPN.

- Define requirements; develop designs, implement prototypes, and support pilots for VPN.
- Provide appropriate training on the use of the VPN.
- Develop an implementation schedule that will ensure distribution of software/devices to all of ICE personnel and locations as required to have an effective implementation.
- Support the implementation of the technology

4.23.6 Government Network

The General Services Administration, at the request of the Executive Office of the President of the United States, and the newly designated Advisor for Cyberspace Security, and in support of National Security goals established by the President, is presently seeking information from industry that will assist in the development and deployment of a special telecommunications network, GOVNET.

GOVNET will be a private Internet Protocol (IP) network shared by government agencies and other authorized users only. GOVNET will provide connectivity among users to a defined set (to be determined) of service delivery points.

There will be no interconnections or gateways to the Internet or other public or private networks. This applies to any network management, control, and maintenance functions for GOVNET as well. Initially, GOVNET will provide private intranet data connectivity within the contiguous 48 United States (CONUS).

The Contractor shall monitor the status of the GOVNET initiative and make recommendations on acquiring the service to support the ICE telecommunication requirements.

4.23.7 Demilitarized Zone – DMZ

A DMZ is a network segment behind your firewall, accessible from the Internet, but a separate network portion from your corporate network. It requires different levels of access than other network components. The general philosophy is that any system on the DMZ can be comprised because it's accessible from the Internet, while the corporate network remains protected.

To support this activity, the Contractor shall:

- Make recommendations addressing the capability of the DMZ to serve as a measure of protection for ICE systems.

4.24 SECURITY OPERATIONS ~~– DELETED~~

The ICE C&TS program requires a centralized capability to manage all related IA security solutions that are deployed and operational. This should include, but not be limited to. Secure Remote Access, DMIC PKI Infrastructure, and other Security operations Technologies as implemented and directed by the ISSM and/or Task Manager.

4.24.1 Access and Data Security

All IA policies stress the need for good identification and authentication (I&A) processes and procedures as one means of helping to ensure the confidentiality, integrity and availability of its information and systems. A strong role and rules based program that operates of the principles of "least privilege"," need to know", and "separation of duties" are three tenets that must be vigorously applied and enforced across the ICE IT infrastructure and on the various systems and components that comprise that infrastructure.

4.24.2 Digital Management Identification Center

DHS policy requires the application of strong authentication and encryption technologies for protecting department IT systems. This project encompasses the acquisition of physical cryptographic tokens, hardware devices and software to facilitate the use of strong authentication. These cryptographic technologies and techniques can be used to support the encryption of local data and any data files transmitted over the ICE WAN or local GSS.

The OISSM Task Order Support Team will coordinate, at the direction of the Task Manager and/or the ISSM, the construction, build-out, and configuration of a new DIMC facility, housed within a Government owned facility, to become the primary DIMC and convert the existing to the backup operational DIMC to support digital identity programs for all ICE components and, as directed, DHS and its other organizational elements. They will also staff, manage, and administer the operational functions of the DIMC.

The DIMC will contain sufficient space to house the following critical elements for administering PKI and cryptographic technologies throughout the DHS:

- Systems Administration Room—The space in which PKI security administrators and technologists conduct 24x7 administration and monitoring operations of PKI elements
- Server Room—Secure location for the PKI technical components (e.g., Security devices and AIS).
- Vault—Houses the Certificate Authority (CA) for the DHS public key infrastructure and other sensitive systems and items. The CA is the critical element in the DHS PKI and is used to generate and backup cryptographic keys and electronic credentials that uniquely identify personnel and are used to encrypt/decrypt sensitive data.

To implement the DIMC, the ICE OISSM Support Team will:

- As directed, Prepare a detailed program plan that identifies key activities, deliverable, and milestones necessary for implementing a secure facility that will provide PKI support capabilities.
- As directed, Prepare a physical design document that includes:

Physical layout and construction

Environmental requirements; e.g., power, Heating, Ventilation, and Air Conditioning (HVAC)

Access controls

Surveillance and detection systems

Alarms

Primary and secondary data and voice communications

Exclusion areas

Secure storage containers

Equipment and Software

Networks

Furnishings

- As directed, prepare the Bill of Materials and cost estimate for build out of the DIMC
- As directed, construct the facility at a location to be determined by the Government
- As directed, provide weekly status reports until construction is completed
- Coordinate, through the ICE ISSM and/or Task Manager, a transition plan to assume responsibility for assuming the daily operations of the existing DMIC facility and PKI infrastructure from the incumbent Contractor support team.

Once a DMIC facility is operational, the Contractor shall:

- Develop and Deliver presentations/demonstrations; provide interface, coordination, and liaison with ICE, ICE Contractors, and external ICE partners; and support ICE participation in Steering and Working Group for PKI technologies, as directed.
- Assist ICE in defining a high-level business case for developing PKI policy, establishing an implementation strategy, and tracking DHS and Federal policies.
- Design and engineer, and build as directed, a DMIC facility to house an ICE PKI Infrastructure;
- Staff and operate a DMIC facility to meet the ICE Mission and operational requirements as agreed by the ICE ISSM and /or Task Manager;
- Support the design and development of the PKI to meet ICE and DHS security architecture. It must:

    1. Have strong security mechanisms that can provide adequate protection of ICE information and systems both now and into the foreseeable future, including the use of public key and secret key cryptographic technologies.

2. Support multiple levels of trust/assurance as required by the ICE mission.
3. Provide integrated, interoperable security services to ensure security: across the infrastructure, including workstations, servers, mainframes, ICENET, ICE LANs, the Internet, intranets, extranets, and remote access; between applications and application components; and between ICE and external partners, including other DHS components, and ICE clients; and provide security services, including digital signatures, to enable the conversion of paper-based processes to electronic-based processes, including electronic commerce activities.
4. Support remote and mobile users.
5. Provide users a single strong means of authenticating themselves to systems and applications, replacing the need to deal with multiple passwords and support role-based access control.
6. Implement a single standard approach to providing cryptographic services for use by all systems and applications to ensure cost effective, uniform support for specific levels of trust/assurance enterprise-wide.
7. Provide efficient, centralized management of IT security including: management of cryptographic keys; secure remote administration of architecture components; management of access controls; vulnerability scanning; collection and analysis of audit information; and intrusion detection.
8. Minimize user interactions required to perform security functions and be reasonably transparent to users.

- Assist in developing a high level ICE Security Policy Statement governing PKI and developing policy statements governing the PKI components.
- Track DHS and Federal Government policies and requirements with respect to PKI components and work to bring the PKI into compliance, or provide support for the preparation of waiver requests, as directed.
- Based on the results of the CSI Pilot , make appropriate changes to related policy, practices, design, etc, to prepare for full-scale implementation. The Contractor shall support the implementation efforts as determined by the ICE ISSM and/or Task Manager. These include:

1. Procure cryptographic tokens, hardware devices, and software to support encryption of local data and data files transmitted over ICE WAN or local GSS.
2. Identify cryptographic application(s) that will protect laptop computers from unauthorized access and compromise through the use of encryption technologies.
3. Procure, install, and maintain cryptographic application(s) that will protect laptop computers from unauthorized access and compromise.
4. Develop an implementation schedule for modifying legacy assets.

4.25 CONTINUITY PLANNING FOR ICE CRITICAL ASSETS

PDD-63 establishes requirements for protecting the nation's critical infrastructure. Critical infrastructures are those physical and cyber-based systems essential to the minimum operations of the economy and government. They include, but are not limited to, telecommunications, energy, banking and finance, transportation, water systems and emergency services, both governmental and private. The DHS has developed a CIP Strategic Plan that is intended to fulfill the President's goals and satisfy the requirements of PDD-63 and later guidance

The ICE is dependent on a large number of automated systems, applications, facilities, and equipment for its operation. Degradation of system operations and/or functionality could debilitate mission-critical functions and operations. The ICE is engaged in adopting protective measures to ensure sustained operation of systems and equipment that will be considered vital to mission performance. Continuity of Operations Planning (COOP) must be accomplished by the various ICE component's Senior Management personnel to identify their minimal essential functions, personnel, and related support requirements. Including IT systems As this is accomplished, the ICE OCIO and ~~C&TS~~ OISSM will be able to help to identity, plan, document, and test the necessary IT contingency Plans for the ICE Major Systems and GSSs as necessary.

ICE cannot expect to effectively recover from a disaster situation in a timely fashion without enduring major disruption to business functions and operations with first having Disaster Recover/Contingency Plans for every site or system. Disaster Recovery/ Contingency Plans provide the basis for the following key elements:

Planning. Establishing backup procedures, forming a disaster management team, pre-planning acquisition requirements, pre-positioning supplies, and establishing agreements with external organizations for the use of facilities and other critical resources.

Response. Developing a disaster notification process, establishing a model for assessing the damage to a facility/site and its physical, personnel, and information technology resources.

Recovery and Restoration. Developing specialized teams to address recovery of existing resources and restoring operations, including prior service levels and functionality, within a reasonable timeframe. Teams will include:

- Disaster Management Team to oversee recovery operations,
- Damage Assessment Team to analyze the situation and determine the overall disaster impact,
- Operations Team to reestablish technical services such as telecommunications interfaces,
- Logistics Team to provide inventory management and transportation services,
- User Support Team to interface with the user community,

- Security Team to secure the site and facility, and the
- Administrative Services Team to provide general support such as clerical and acquisition activities.

Policies underpin an organization's whole approach to contingency and disaster recovery. They determine the fundamental practices and culture throughout the enterprise. They are usually linked closely with information security policies and also address the basic defense requirements to ensure the stability and continuity of the organization. It is essential therefore that they exist, are up to date and are comprehensive in their coverage.

The Contractor shall:

- Ensure that the necessary COOP, CP, and DRP policies and procedures are adequately addressed within the ICE ~~C&TS~~ OISSM policy documents, handbooks and procedures.
- For every DRP/CP document created or reviewed, ensure that the following are adequately addressed:
    1. Potential impacts of each type of disaster or event.
    2. Risks and their magnitude of the scenarios most likely to occur.
    3. That minimal essential resources are clearly identified;
    4. That a personnel succession plan is completed
    5. That all aspects of continuing operation are addressed.
    6. That continuous review/audit of the plans is addressed to ensure that the plan remains current and stands up to rigorous examination
    7. That the plans addresses the need for reports of reviews and testing on a regular basis in accordance with DHS or higher authority
    8. Prepare and submit reports that cover lessons learned during testing of or reviews of an CP or DRPs.
- Develop and maintain the ICE CIP plan and ensure it is in compliance with the DHS CIP plan.
- Update the ICE HQ (facilities) Emergency Response Plan as requested by the ICE ISSM and/or Task Manager. This document was prepared in the 1st quarter of 2002 and will be regularly updated, as required.
- Develop an ICE Disaster Recovery Plan (DRP) that will address regeneration of mission critical OCIO resources in the event of a disaster or other emergency. This document will include procedures necessary for the regeneration and relocation of ICE Headquarters activities
- Develop an ICE OCIO Disaster Recovery Plan that will address all OCIO services, capabilities, and functionality, including the Network Operations Center (NOC), SOC, and the ICE Help Desk. Responsibility for disaster recovery planning for operational

facilities such as the ICE SOC, NOC, and Help Desk, will be coordinated with the current IT operations support Contractor.

- Prepare and/or assist, other contingency planning and disaster recovery planning materials as directed by the ICE ISSM and/or Task Manager.

4.26 NATIONAL SECURITY SYSTEMS (NSS) AND COMMUNICATIONS SECURITY (COMSEC) MANAGEMENT

The ~~C&TS~~ OISSM Program Office is responsible for managing the security of ICE IT systems that process National Security Information (NSI) or "Classified" data processed or stored on any ICE computer, GSS, and major systems/applications, regardless of physical locations, and operated by ICE organizational components

The Contractor shall:

- Provide qualified staff who are cleared up to and including the Sensitive Compartmented Information (SCI) level to support NSI program requirements
- Provide assistance in the development of security policy for ICE NSI systems
- Preparation and maintenance of a NSI Systems Project Management Plan. This document will describe procedures to meet policy requirements, define the scope of the project, define actions and objectives, and provide milestones necessary for achieving goals and objectives
- Acquire, install and maintain the necessary DHS or higher authorities requirements for processing NSI information in the performance of this tasking. This capability shall be in Government spaces approved for the processing of NSI data.
- Provide support for ensuring that ICE requirements for the DHS HSDN are clearly identified and communicated;
- Provide engineering and technical design support for interfacing with the DHS HSDN;
- Develop transition plans for ICE NSS to transition/connected to the DHS HSDN
- Management of NSI system security plans and activities in a physically secure environment where necessary
- Preparation of the classified and unclassified Certification and Accreditation documentation necessary for authorizing NSI system operations in the ICE, DHS and other NSI environments in accordance with approved procedures and directives
- Implementation of an awareness program that addresses the special needs of the community responsible for NSI systems. The NSI awareness program will be included in the Awareness activities described in Activity 2.4
- Coordination of an appropriate security-related training syllabus. Training information will be included in the Information Security training Plan submitted as part of Activity 2.4

- Coordination and preparation of ISAs when connectivity requirements dictate
- Ensuring that appropriate project status information and progress data are maintained and made available for required FISMA reports
- Providing subject matter expertise in discussions with organizations both within and outside ICE regarding NSI security matters
- Coordination of NSI system security incident reporting. Incident reporting will conform to the requirements of the ICE CSIRC reporting procedures
- Conduct site visits to assist the ISSO in planning for and meeting NSI security requirements as part of the ISSO Support in activity 2.3.1
- Provide support to ICE component operations in the development and maintenance of local security procedures in support of NSI system security
- Provide support to the ICE ISSM to ensure program compliance
- Serve as the ISSM representative to other organizational elements in support of ICE NSI security initiatives
- Provide support and guidance to DHS Organizational Elements under a shared resource concept
- Serve as a member of working groups/configuration management bodies
- Develop system lifecycle capabilities for NSI systems to include configuration management and change control
- Coordinate with the NSS System owners, ICE Customer Service Branch and Infrastructure Engineering Branch to develop a CIO/OCIO plan for assuming and providing all Operations and Maintenance support for all ICE NSS regardless of locations
- Coordinate with NSS systems owners to bring all NSS under a ICE CIO NSS centralized Configuration Management plan and processes, where feasible.

TASK E – UNIX SYSTEMS SUPPORT & DATABASE ADMINISTRATION (TORP SECTIONS 4.27 THRU 4.28)

The purpose of this Task Order is to describe the task activities, scheduling, staffing resources, management and technical approaches related to the UNIX Systems Support Task Order of the United States Department of Homeland Security (DHS) Bureau of Immigration and Customs Enforcement (ICE) Service Technology Alliance Resources Systems Management and Integration (SMI) contract.

The ADP Operations Branch (HQAOB), UNIX Systems Support Section is responsible for the evaluation, selection, and implementation tasks associated with obtaining and integrating new UNIX operating system software, solving operational problems involving UNIX operating systems software, designs, implements and monitors equipment software performance and support programs for systems supported by the ICE Bureau of the DHS.

UNIX Systems Support provides environmental support for the UNIX development, test, and production systems. This includes the operating system as well as system maintenance, upgrades, fixes, patches, tools, and new releases. Many, if not most, of the applications that run on these systems are DHS mission-critical that must be operational 24 hours a day, seven days a week.

ICE is working toward creating a more homogeneous UNIX environment. Currently, there are over 40 Oracle databases running on IBM and Siemens UNIX platforms. The goal is to migrate all Oracle production databases to IBM AIX/UNIX platforms.

With increased public scrutiny and greater resource demands on DHS operational components, the ICE Office of Information Resources Management (OCIO) must utilize the most effective means to automate the management of information and provide productivity capabilities to operational programs. Specifically, the ICE and its Contractors need a clear understanding of:

- The UNIX/Oracle databases currently in ICE possession, and their structures
- UNIX based systems likely to be acquired or created by ICE in the near future
- The probable evolution of ICE UNIX systems in view of technological advances
- Potential difficulties involved in migrating from one platform to another
- Methods of maintaining operating system integrity and security
- Hitachi Storage Area Networks
- Administration of Backup Software
- Tracking of vendor maintenance and support agreements
- ICE System Development Life Cycle (SDLC)
- Web sphere MQ Series

4.27 TASK MANAGEMENT AND COORDINATION

The Contractor shall prepare weekly and monthly status reports for the United States Department of Homeland Security (DHS) Bureau of Immigration and Customs Enforcement (ICE).

4.27.1 Technical Guidance and Support

The Contractor shall provide technical support for the system administration of UNIX databases and application servers utilizing web-based, client-sever and/or host-based applications. In addition to the aforementioned, the Contractor shall perform the following activities:

- Provide UNIX system administration and database support
- Monitor application and database servers and troubleshoot/resolve OS and MQ Series issues
- Verify that the production and development servers are operational
- Install and administer all operating systems and software associated with the servers including back-ups, fixes, patches, tools, etc.

- Provide 24 x 7 problem resolution and support.
- Coordinate OS upgrades, patches, fixes, and testing with Data Center staff

4.27.2 Environment Configuration

The Contractor shall provide configuration, tuning, and maintenance of UNIX operating systems on IBM AIX/UNIX servers. When the IBM AIX servers have been configured, stabilized and certified for production use by ICE, the Contractor shall support the migration of each database environment from other platforms to the IBM/AIX environment on an "as-needed" base. The configuration required at the DOJ Data Center in Rockville, MD shall include (at a minimum):

- 6 IBM M-80 servers
- 2 IBM p660 servers
- 4 IBM P690 (Regatta) Servers

The configuration required at the DOJ Data Center in Dallas, TX shall include (at a minimum):

- 1 IBM M-80 server
- 1 IBM P660 server
- 2 IBM P690 servers

4.27.3 Performance Monitoring

The Contractor shall continue to monitor the performance and provide disk management and control for UNIX databases and application servers to ensure optimal performance.

4.27.4 Maintain UNIX Documentation

The Contractor shall create/maintain and updates the following documentation:

- Startup/shutdown procedures for all UNIX production and database servers
- Allocation of disk storage procedures for all UNIX production and database servers
- User ID procedures for all UNIX production and database servers
- AIX/UNIX Application Development Guidelines and Procedures

4.27.5 System Administration/Capacity Planning

The Contractor shall provide expert knowledge in capacity planning of UNIX servers. The Contractor shall provide:

- Analysis of ICE plans
- Develop workload projections
- Prepare a semi-annual Capacity Planning Report
- Monitor systems usage
- Advance notice of storage increase requirements

- Efficient maintenance and tracking of storage

4.27.6 US VISIT Support

The Contractor shall support the development, testing and implementation of the USVISIT databases and interconnects within the defined scope of this task.

4.27.7 Data Center Relocation/Database Migration

The Contractor shall support the planning and relocation of all ICE UNIX-based platforms from the two DOJ data centers to the two DHS data centers. The Contractor shall coordinate data migration with Database Administrators. Data Center relocation is expected to occur in fiscal year 2005.

4.27.8 Maintain UNIX Documentation

The Contractor shall facilitate and support the establishment and maintenance of MQ Series queues hosted in centralized ICE UNIX-based servers.

4.28 TASK MANAGEMENT AND COORDINATION

This plan describes support that will be provided to the DHS in the areas of Management, Coordination and Database Administration; including Oracle Environment Configuration, Oracle Name Server Maintenance, Database testing, MQ Series support, US VISIT Increment 1 system support, and Data Center relocation and Database Migration support.

The Department of Homeland Security (DHS) is working to make effective use of information technology (IT) by developing and implementing information systems that improve access to information across the Department and other Federal, state, and local law enforcement entities. The Bureau of Immigration and Customs Enforcement (ICE) is taking a proactive position in integrating and modernizing its databases, and ensuring that newly developed software and databases are maintainable, and easily transitioned to newer platforms. The currently ongoing integration of USVISIT, ADIS, and IBIS advances these mission objectives through automating the sharing and integration of information within the DHS and state and local law enforcement agencies. ICE is nearing completion of the integration a myriad of specialized databases into a unified, comprehensive Enforce Integrated Database (EID). Utilizing its database integration experience, ICE is providing a leadership role in demonstrating the means of integrating the many diverse databases across the DHS. At present, ICE has a disparate information environment containing mainframe, client/server, and web-based application environments. There are approximately 30 IDMS "national databases" that run on the IBM z/OS operating system, and over 40 Oracle Production databases that run on IBM UNIX platforms. Primary among these are the Claims 4 database and the ENFORCE Integrated Database utilizing Oracle RAC on the AIX/UNIX operating system. Oracle databases remaining on the Siemens platform are scheduled to migrate to IBM utilizing AIX operating system.

With increased public scrutiny and greater resource demands on DHS operational components, the ICE Office of Information Resources Management (OCIO) must utilize the most effective

means to automate the management of information and provide productivity capabilities to operational programs. Specifically, the ICE and its Contractors need a clear understanding of:

- The databases currently in ICE possession, and their structures
- Databases likely to be acquired or created by ICE in the near future
- The probable evolution of ICE databases in view of technological advances
- Potential difficulties involved in migrating data from one database to another
- Methods of maintaining data integrity and security
- Maintaining databases for other Bureaus
- Incorporating legacy databases from incoming ICE components into ICE standard platforms while maintaining support for these databases
- Configuring and maintaining Oracle Real Application Clusters (RAC) in a partitioned IBM AIX environment using High Availability Clustering (HACMP)

The Contractor shall provide full software development life cycle (SDLC) and data management support services as required to meet the overall objectives of the task and will continue to provide an integrated and controlled approach to the database management and technical support services. The Contractor has the primary responsibility for ensuring that the products/services meet the performance and design requirements specified in accordance with this TORP. The Contractor is considered to have expertise in the tasks identified in this TORP. In consideration of this expertise, the Contractor shall notify, in writing, the ICE Contracting Officer's Technical Representative (COTR) of any omissions or clarifications that will enhance the TORP in order to provide a better solution for the U.S. Government. The Contractor shall provide:

- An integrated and controlled approach to the management of DHS vital data resources
- Support the infusion of application support technology
- Technical assistance to ICE organizations
- Operational support for the definition, maintenance, security, and integrity of some non-ICE databases
- A Balanced Scorecard concept of interpreting/displaying the results of the established performance measures
- Services consistent with those of skilled Database Administrators
- Database integrity though security standards as prescribed by DHS 4300b

4.28.1 Purpose

The Contractor shall provide:

- Reports summarizing security activities related to the database server log ins

- Graphical reports that demonstrate database server processor utilization, session activity, and operational statistics
- Monthly reports relevant to the support of the database systems and servers
- Weekly reports describing specific DBA activity for that week

4.28.2 Guidance

The Contractor shall provide technical support for the identification, development, and establishment of ICE policy, standards, procedures, and guidelines. In this capacity, the Contractor shall review Federal, State, and Local guidance, as well as, commercial standards for their impact on the ICE computing architecture. The Contractor shall update Oracle Application Development Guidelines, IDMS Application Development Guidelines and Procedures, and MQ Series Standards Guidelines documents at least once per year, or more frequently as policy or technology shifts dictate. The Contractor shall review and provide recommendations for addition or changes to the ICE System Development Life Cycle (SDLC) document once per year or as new versions are produced.

4.28.3 Database Administration Support

The Contractor shall provide database administration support for all ICE applications, and any other databases as determined by the Government. This includes all database administration activities required to provide accessible, secure, and dependable databases for ICE. The activities include:

- The creation and maintenance of database structures for IDMS and Oracle
- Maintenance of standards and procedures for distributed Oracle databases
- Maintenance of standards and procedures for IDMS databases
- 24 x 7 database support and problem resolution
- Database performance and tuning
- IDMS and Oracle security requirement and solutions
- Application design reviews
- Enterprise scalability analysis plans for IDMS and Oracle systems as requested
- 12 x 5 database support and problem resolution for SQL Server databases

4.28.4 Oracle Environment Configuration

The Contractor shall provide configuration, tuning, and maintenance of Oracle databases on IBM AIX/UNIX servers. When the IBM AIX servers have been configured, stabilized and certified for production use by ICE, the Contractor shall support the migration of each database environment from other environments to the IBM/AIX environment on an "as-needed" base. The configuration required at the DOJ Data Center in Rockville, MD shall include (at a minimum):

- 6 IBM M-80 servers
- 2 IBM p660 servers
- 4 IBM P690 (Regatta) Servers

The configuration required at the DOJ Data Center in Dallas, TX shall include (at a minimum):

- 1 IBM M-80 server
- 1 IBM P660 server
- 2 IBM P690 servers

4.28.5 Oracle Name Server (ONS)

The Contractor shall maintain at least 4 regional ONSs' in accordance with Oracle standards and ICE security policy. Each ONS will be configured to accommodate up to 40,000 named users.

4.28.6 Database Testing

The Contractor shall configure environments for, and support all database related aspects of user acceptance testing, functional acceptance testing, database testing, installation testing, configuration/compatibility testing, security testing, and performance, load and stress testing.

4.28.7 US VISIT Increment 1 Support

The Contractor shall support the development, testing and implementation of the US VISIT databases and interconnects within the defined scope of this task.

4.28.8 DATA CENTER RELOCATION AND DATABASE MIGRATION SUPPORT

The Contractor shall support the planning and relocation of all ICE databases from the Rockville, MD and the Dallas, TX DOJ Data Centers to the two new DHS-ICE Data Centers. The Contractor shall play a lead role in migrating data from the DOJ Data Centers to the new DHS Data Centers. This migration is expected to occur in fiscal year 2005.

4.28.9 Support ICE Operations

The Contractor shall provide support for the OCIO section of ICE. This support includes:

- Manage, support, and maintain integrity of the ICE legacy data entities
- Specify guidelines for accessing business data
- Maintain data structures and operating systems
- Support each phase of the SDLC
  - Planning and Requirements Phase
  - Design Phase
  - Development and Testing Phase
  - Implementation Phase
  - Development, Testing, Training Database Support
  - Production Database Support

TASK F – IT INFRASTRUCTURE MANAGEMENT SUPPORT (TORP SECTION 4.29)

Systems Management and Integration (SMI) Contractor shall assist the Office of the Chief Information Officer (OCIO), in organizational planning and implementation, ICE transition planning and implementation, Program management assistance, and Contractor oversight support. Organizational planning and implementation includes analysis of current processes and procedures, process re-engineering activities to support Business Lines, assistance in planning for internal restructuring, and developing organizational communication strategies. ICE transition planning and implementation includes assisting in data gathering and responses to ICE action items. Program management assistance includes support to respective program/project managers in tracking Contractor performance, management and financial analysis, and organizational change management. Contractor oversight support includes coordination and Contractor oversight in the areas of deployment, and financial tracking and analysis.

OCIO anticipates continuing to deploy and upgrade the technology infrastructure throughout Fiscal Years 2004 and 2005 consistent with program priorities. As this deployment proceeds, and the infrastructure continues to grow in scope and complexity, continued planning will be required to sustain capacity and performance. Methodologies, tools, and procedures must be implemented to manage and control system and network resources and assets. New and emerging technologies must continue to be assessed as a force multiplier for implementation where applicable.

The Contractor shall provide management and technical support to the Systems Integration Division by:

- Assisting in the planning and management of the transition of personnel and assets to ICE;
- Facilitating the installation and upgrade of consistent and compatible hardware, software, and communications platforms, including custom applications deployment expeditiously as possible according to program priorities;
- Identifying problems through communications with Government staff and other Support Contractors and proposing solutions;
- Facilitating the tracking, management, and accountability of all Information Technology (IT) assets; and
- Supporting the individual project managers within ICE by providing management, analysis and financial analysis support.

4.29 TASK MANAGEMENT

The Contractor shall be responsible for the effective management and administration of all efforts undertaken under this Task Order. The Contractor shall identify and maintain a management structure and organization with overall project control and authority for the performance of work under the Task Order. The Contractor's management structure and organization shall ensure that the following requirements, at a minimum, are satisfied throughout the life of the Task:

- A technically proficient and professionally capable staff is established and maintained; Personnel turnover is minimized and individuals are motivated to achieve excellent and timely performance;
- Problems are avoided and unavoidable/unanticipated problems are resolved with little or no disruption to the activities performed under the task order;
- Feedback on performance is obtained from Government management and provided to Contractor personnel on all areas of task order performance;
- Quality and timeliness of the products and services provided under this task order are continually monitored to ensure improvement; and
- All resources used for the performance of work under the task order are identified, their roles clearly defined, and their relationship to the remainder of the organization established and identified.

ICE requires an operating environment that embodies a combination of quality, cost-effectiveness, industry best practices, efficiency, and flexibility. The Contractor shall review industry best practices and develop an operating framework, customized to the environment, to optimize the productivity of the ICE Team.

4.29.1 Task Management Reporting

The Contractor shall maintain detailed resource assignment data, tracking individual task status, problems, issues, progress, and other activities related to this Task Order. The SMI Task Leader shall be able to accurately describe project and task status, including resources utilized (by name), significant accomplishments (milestones achieved, quantities of inputs processed, etc.), problems or issues encountered (by task activity), resolution steps, costing data and burn rates (by task activity), and various other data as required.

The Contractor shall submit a monthly Task Order Progress Report and a Monthly Task Order Financial Analysis Status Report as required by the Contract. The Task Order Report shall discuss the status of the task (generally), and each task activity (specifically), and shall include:

- Progress since last reporting period;
- Outlook or plans for the next reporting period; and
- Issues that the SMI Contractor believes require near-term Government Task Manager intervention in order to forestall potential progress delays.

In addition to these reports, the Contractor shall hold monthly Task Order Management Review meetings with the Government Task Manager(s) and designees. The Contractor shall prepare agendas and handouts for status meetings. The Contractor shall define action items by task activity that require Task Manager attention, action items requiring SMI attention, dependencies or issues that prevent progress, summaries of achievements, trends or performance issues or recommendation that would improve quality, or similar information.

4.29.2 Quality Assurance/Control Requirements

The Contractor shall ensure consistent technical quality of deliverables, work products, and services provided utilizing quality assurance/control measures.

TASK G - TECHNICAL REQUIREMENTS - OPTIONAL TASK (TORP SECTION 4.30)

4.30 TECHNICAL REQUIREMENTS

4.30.1 Portfolio Level Management Support

The Contractor shall assist in providing overarching, objective, and analytical management support, working closely with the ICE OCIO Program Managers as well as other Program Managers. The Contractor shall conduct organizational planning and implementation assistance to include analyzing and documenting current processes and procedures, performing process re-engineering activities to support Business Lines, providing assistance in planning for internal restructuring, and developing organizational communication strategies. Contractor shall assist in DHS transition planning and implementation by assisting in data gathering and assisting managers with development of responses to DHS action items. Contractor shall provide Program management assistance including support to respective program/project managers in tracking Contractor performance, management and financial analysis, and organizational change management. The Contractor shall track, coordinate, and ensure the timely completion of high visibility projects. The Contractor shall assist with the initiation and review of draft correspondence and responses to queries and taskings from outside ICE OCIO for accuracy, consistency, and completeness. The Contractor shall attend meetings as directed, and provide analytical support to the ICE OCIO point of contact (POC) relative to the subject matter of those meetings. The Contractor shall conduct objective and independent analyses and assessments of ICE OCIO functions and operations as directed by the Task Manager. The Contractor shall assist in defining, collecting, and consolidating organizational performance measures.

The Contractor shall provide assessment and monitoring of organizational functions and activities within ICE OCIO. The Contractor shall monitor change within the organization to identify weaknesses or inconsistencies that exist. The Contractor shall monitor the integration of functions and responsibilities within the organization and with other entities within ICE OCIO and within DHS. The Contractor shall monitor the quality of work being accomplished and of the functioning of the organization as a whole, identifying duplication of effort and developing and recommending alternative solutions to negate the overlap. The Contractor shall periodically review status reports and deliverables submitted by the Deployment Contractor to assess and verify the accuracy of information being collected throughout the organization and continuously review the accuracy of performance and statistical data being entered into infrastructure databases. The Contractor shall track ICE OCIO credit card accounts and purchases. This includes working with purchasers to resolve issues with orders as received, and completing monthly reconciliation of the bank statement.

4.30.2 Technology Infrastructure Management Support

The Contractor shall provide support to facilitate the installation and upgrade of all identified hardware, software, and communications platforms at identified sites. This support includes, but is not limited to, providing management oversight support for all aspects of infrastructure deployments to ensure consistency, and responsiveness in accordance with mission objectives. The quality assurance/control shall include technical reviews and audits to validate the quality of the work performed by the Deployment Contractor personnel.

The Contractor shall assist in the management of infrastructure activities, including planning, oversight, and acquisition support of infrastructure activities. Required support includes the following activities:

- *Planning and Task Coordination Assistance* - The Contractor shall analyze, design, and generate a web-based tool to display all relevant infrastructure related activities and documentation;
- *Project Tracking Support* - The Contractor shall analyze, design, and maintain a comprehensive project tracking system for all infrastructure related activities; this includes generating and tracking Service Level Agreements (SLAs);

IT Acquisition Review -. The Contractor shall provide technical review of Automated Information System (AIS) requests and report statistics on a weekly, monthly, and as required basis.

4.30.2.1 Planning and Task Coordination Assistance

The Contractor shall analyze, design, and generate a web-based tool to display all relevant infrastructure related activities and documentation. This tool shall display data in a variety of formats with appropriate security for each level of display. The Contractor shall work with the Deployment Contractor to ensure that data related to current and upcoming activities is able to feed into this tool for real-time display of information. The Contractor shall perform the following activities as required:

- **Requirements and Business Process Improvements**
  - Document customer specifications and interact with other support groups to identify business processes, systems, and product requirements; and
  - Evaluate unanticipated problems and or emergencies as they occur and explore and recommend solutions.
- **Coordination and Communication**
  - Provide coordination and documentation support for meetings hosted by OCIO, ICE, or other DHS personnel;
  - Prepare meeting minutes, issues, and action items; track each issue and action item through its resolution as approved by the Task Manager;

- **Infrastructure Technical Assessment and Configuration Recommendations**
  - Assist in the technical evaluation of new and emerging technologies that may be applicable to the technology infrastructure at DHS;
  - Coordinate with Infrastructure management, Application Project Managers and the Infrastructure Deployment Contractor to address technical issues that may arise, which may impact infrastructure equipment operations;
  - Attend and participate in Architecture Review Board meetings as requested.
- **Clerical and Administrative Support**
  - Provide clerical and administrative support;
  - Track Other Direct Cost (ODC) requests submitted by Deployment Contractor.

4.30.2.2 Project Tracking Support

The Contractor shall analyze, design, and maintain a comprehensive project tracking system for all infrastructure related activities; this includes generating and tracking Service Level Agreements (SLAs).
The Contractor shall support ICE in tracking and reporting on all deployment activities related to the technology infrastructure.

- **Deployment Tracking and Reporting**
  - Coordinate and monitor deployment activities, including pre-site and site surveys; deployments, and post-deployment support;
  - Identify and design standardized periodic and ad-hoc reports tailored for varying levels of management, to include Infrastructure personnel, OCIO Senior Management, and others as required;
  - Prepare and distribute periodic (such as the Monthly Deployment Status Report) and ad-hoc status reports identifying in-progress, upcoming and completed deployment activities; and
  - Prepare and maintain briefing and presentation materials as required by ICE management to convey information to Management and/or oversight organizations, agencies or groups.
- **Budget and Financial Assistance**
  - Assist in generating and maintaining Service Level Agreements and monthly financial tracking in support of reimbursable and Operations and Maintenance (O&M) Infrastructure activities.
- **Database Administration and Maintenance**
  - Update the Refresh Cost Model;
  - Provide ad-hoc assistance as required for developing and maintaining database tools in use within ICE.
- **Processes and Procedures**
  - Maintain Standard Operating Procedures (SOPs) for the Infrastructure Branch;

- Maintain workflow diagrams for deployment life-cycle activities; provide updates as requested;
- Assist in the development of SOPs based on knowledge of Branch operations.

4.30.3 IT Acquisition Review Support

The Contractor shall assist in review, coordination, and liaison support of Infrastructure acquisition activities. Specifically, the Contractor shall:

- Provide centralized support in the acquisition of infrastructure hardware and software, equipment requisition tracking, and validate shipments into Staging to facilitate the invoice payment process;
- Monitor and insist upon accurate inventory inventories of stored goods, receiving activity, staging activity and shipping activity;
- The Contractor shall provide technical review of Automated Information System (AIS) requests and report statistics on a weekly, monthly, and as required basis.

4.30.3 Asset Management Oversight – Deleted

4.30.5 Special Projects

The Contractor shall be available to support Special Projects as required. Typically, these projects will be for a specific Branch within ICE or other DHS entity that is able to provide funding for the specified project. At the writing of this TORP, there are five known projects as detailed below.

4.30.5.1 Technology Training Services (ITS) Branch Mgmt and Financial Support

The Contractor shall provide management support to include planning, tracking, coordinating, and reporting on the various reimbursable training activities. This shall include reviewing, analyzing, and tracking Branch task plans and financial status. The Contractor shall also coordinate with other ICE Branches in order to analyze and cost their training needs and review all requirements to ensure that they are included in Atlas projections for FY04-FY08. The Contractor shall attend meetings, as required, to determine customer requirements and communicate them to TTS personnel. The Contractor shall prepare written and verbal reports and briefings, as required, and will provide assistance with drafting correspondence, justifications, and responses to queries from outside entities. The Contractor shall review and analyze training vendor cost estimates, actual costs, and clients' account balances. The Contractor shall provide analysis and research on technical and organizational topics as they relate to training, learning, and knowledge.

4.30.5.2 ADP Operations Technical Support

The Contractor shall provide data analysis support for the System Access Rights Review (SARR) project. This support is anticipated for three months.

4.30.5.3 Integrated Automated Fingerprint Identification System (IAFIS) Project Support

The Contractor shall attend IAFIS related meetings, capture and submit meeting minutes via e-mail, and follow up on all outstanding action items. Action item status reporting shall be done once per week, also by e-mail. All site survey information shall be captured and analyzed for issues that need to be resolved. Issues shall be forwarded as they are received, to the Deployment Manager. This support is anticipated for twelve months.

4.30.5.4 Customer Service Branch Support

The Contractor shall assist the Customer Service Branch in identifying, analyzing, and documenting procedures within the Branch. This includes, but is not limited to the following:

- Assist in developing cross-component DHS Help Desk Procedures
- For software products – document procedures for life-cycle support (from product assurance acceptance to deployment in the field, to help desk support, and Operations and Maintenance through retirement)
- Analyze and document other processes within the Customer Service Branch as required

4.30.5.5 Computer and Telecommunications Security

Support the following activities: Requirement Analyses, COTR and Program coordination, Analyze Data, Database Management, Inventory Maintenance and limited Administration duties.

The Contractor must:

- Coordinate with the contract COTRS to collect contact user data
- Coordinate with application program managers to collect data.
- Analyze and review gathered data
- Create, maintain and analyze reports
- Manipulate and Maintain the SARR Data Collections Tool
- Work with technical support providing database management and administration.
- Assist the ~~C&TS~~ OISSM Branch management as needed
- Inventory Maintenance – Respond to Bi-yearly Inventory Calls. Input the ~~C&TS~~ OISSM Branch Equipment into the inventory systems AMIS and ITT. Bi-weekly monitor new equipment and assign a Property Control Number (PCN). Track equipment arrival and destination. Periodically, work with the Excess Equipment Team to excess equipment. Attend occasional meetings.

TASK H - DECISION SUPPORT SYSTEMS (TORP SECTION – 4.31 THRU 4.31.5)

The ICE Office of Chief Information Officer (OCIO), Decision Support Division's mission is to:

- Implement integration of data resources
- Design acquire, and deliver systems that provide information critical to the ICE business decision–making process
- Provide stewardship of ICE Business Intelligence Resource

The basic function of this task is to support the ICE, OCIO, Decision Support Division activities associated with data integration.

The Contractor shall provide operational and administrative support of the ICE Business Intelligence Resource. This includes the set of activities required to ensure smooth daily operations, ensure that resources are optimized, ensure growth is managed, and create, maintain and enforce data extraction, transformation, load, and delivery standards and functions.

The objective of this task is to provide support and to complement the ICE, OCIO, Decision Support Division in order to effectively manage its Business Intelligence resources, which includes the operational data store(s).

All deliverables shall require the review and acceptance of the ICE Task Manager. The Contractor shall submit to the ICE Task Manager a draft deliverable (in electronic format only) for review before the final submittal. The Contractor shall develop all deliverables using the current ICE standard Office Automation (OA) commercial of-the-shelf (COTS) application. Microsoft Office 2000 is the OA COTS standard.

The Contractor will need to coordinate aspects of this task with Database Administrators; computer services staff, application development Contractors and other ICE Contractors. The Contractor also needs to be apprised of related activities being performed under different tasks, and which may have a bearing upon the current task. Travel within the continental U.S. may be involved for coordination and data gathering. No more than four trips outside the greater Washington, DC area with a maximum of two people per trip are anticipated. This task shall make use of ICE SDLC version 6.0, when applicable.

4.31 DECISION SUPPORT

4.31.1 MANAGEMENT, COORDINATION, AND ADMINISTRATIVE SUPPORT

The Contractor shall prepare weekly and monthly written status reports during the execution of this task. Reports shall include a summary of any noteworthy "lessons learned" that might be valuable to this task or related ICE activities. The Government may also direct white-papers/reports to cover special topics relevant to this task.

Management functional roles include:

- Managing associated groups of Operations Data Stores (ODS)
- Manage teams of subject matter experts
- Prioritize requirements

- Schedules tasks
- Communicates progress to Government managers
- Manages scope and expectations
- Coordinates external and internal resources

4.31.2 DATA DESIGN

The Data Design subtask provides and maintains the metamodel for the ICE Operational Data Store (ODPS). This is a standards-based, procedure-oriented function. Communication of these standards to the customer community on a regular basis is essential

Functional Roles include:

- Communicate physical and logical database design to database administrators
- Evolve models to meet new and changing business requirements
- Develop processes for capturing and maintaining metadata from all data integration components
- Maintain compatibility with organized data modeling standards
- Ensure overall health and performance of Operational Data Store (ODS) metadata repository
- Maintain meta model for metadata repository
- Maintain Standard Tables
- Develop and Maintain Standard Table Configuration Management and Change Request Processes

4.31.3 DATA ACQUISITION

This subtask involves the creation and population of the Operational Data Store (ODS). This is where intelligent information integration is performed. Data must be extracted from the source database, transformed into efficient, standard format, and loaded into the ODS. Expertise necessary to perform these functions using a variety of ETL tools and an Oracle ODS is necessary. Source data may be derived from IDMS, Oracle, or other databases. The ODS must then be maintained according to carefully developed maintenance standards. Support for this resource must be available 24/7.

Functional Roles include:

- Ensure overall health and performance of ODS(s)
- Monitor performance, reliability, availability, and recoverability
- Administer user access protocols
- Identify, understand, and coordinate with source data systems and owners
- Map source data to ODS models
- Develop, test, and deploy ETL processes
- Define and capture metadata and rules associated with ETL process

- Adapt ETL process to accommodate changes in source systems and new business user requirements
- Monitor, manage, and validate data warehouse activity including data extraction, transformation, movement, loading, and updating processes
- Ensure the ODS meets service level requirements
- Develop, manage, schedule, and document ODS operations and tasks including extraction, movement, loading, archival, security, backup, and aggregate table creation
- Manage requests for change and prioritizes work based on business needs and available resources
- Defines and documents the technical architecture of the ODS including the physical components and their functionality
- Evaluates, selects, tests, and optimizes hardware and software products
- Estimates system capacity to meet short and long-term processing requirements
- Writes/reviews specifications for client machines, applications/web servers, database servers, and networks

DELIVERABLES	DUE DATES
Decision Support System Lifecycle	First Version within 90 days of Start of contract
Re-hosted database	Software re-hosted per agreed-upon schedule
Utilization Reports, including statistics	Monthly, 15 DARP

4.31.4 DATA ACCESS AND DELIVERY

This subtask is most visible to the end user of Decision Support Systems. End users within ICE are largely comprised of Law Enforcement Professionals and not the general public. Integrated information products delivered to this user base may be of a sensitive nature requiring data security skills. Also, information delivery must be timely in many cases.

Functional Roles Include:

- Write applications/dashboard/dimensional cube mechanisms that let end users access and analyze data in an ODS
- Coordinate with business requirements analysts to understand and prioritize user requirements
- Coordinate end-user training and business-oriented metadata definitions
- Liaison between end-users and ODS project teams
- Determine requirements for data, reports, analysis, metadata, training, service levels, data quality, and performance

- Coordinate with architects to translate requirements into technical specifications
- Identify and assess potential data sources
- Validate ODS
- Coordinate prototype previews
- Maintain library of all associated documentation
- Track versioning of all tools and access methods
- Reviews and edits all documentation
- Develops, maintains, and trains users on Decision Support Systems lifecycle processes
- Reviews and reports on adherence to processes
- Modifies/updates processes in accordance with changes in business requirements, organizational standards, technical architecture, and political/legislative directives
- Ensure that all systems, applications, and tools adhere to DHS security requirements
- Monitor systems for security lapses, loopholes, and attacks
- Build and maintain robust information delivery website

DELIVERABLES:

DELIVERABLES	DUE DATES
Decision Support System Lifecycle	First Version within 90 days of Start of contract

4.31.5 DATA GOVERNANCE

Data Integration cannot occur in a vacuum. Neither can development and extraction of reliable information from data occur without standards, policies, and processes. The Data Governance subtask provides these functions. As stewards of the integrated data resource, data administrators must have detailed knowledge of each data element comprising the Operational Data Store (ODS). Adherence to existing Enterprise Architecture standards and models as well as development and enhancement of existing standards, models, and guidelines are critical functions of this subtask.

Functions under this subtask include:

- Maintain extensive knowledge of business domains with respect to particular data elements

- Provide stewardship of data elements
- Track and interpret communication between business and technical units
- Coordinate and facilitate meetings, seminars, and occasional training sessions
- Document exceptions to governance rules, standards, and procedures
- Proofread all official documentation
- Remove and edit technical jargon from documents intended for business unit consumption
- Ensure that data governance rules, standards, and procedures are followed
- Clearly communicate ramifications of failure to adhere to governance rules, standards, and procedures
- Prepare marketing documents which highlight successes and services provided by the Decision Support Division

DELIVERABLES:

DELIVERABLES	DUE DATES
Updated data architecture Standards	Per agreed upon deliverables
Updates to ICE Enterprise Data Model	As required by changes
Updates to ICE Metadata Repository	As required by changes
Updates to ICE XML Dictionary	As required by changes
Creation and Maintenance of ICE Decision Support Systems Dictionary	First Version within 90 days of start of contract.
Support for and Enforcement of ICE Data Standards	As necessary
Adherence to, Creation for, and Enforcement of ICE Business Rules for Data	As necessary

5.0 INVESTMENT TASKS

The Contractor shall provide services required to develop and/or deploy new functionality or enhancements to existing business functions when approved through the Information Technology Investment Management (ITIM) Process and authorized by modification to this task order.

6.0 TESTING

The Contractor shall comply with Procedures and Documentation requirements outlined in the SDLC Manual. The Systems Assurance Configuration Control Board (SACCB) must approve deviations from the SDLC process by using the Request for Deviation Form.

The Contractor shall perform and participate in the formal reviews set forth in the SDLC. Specifically, a Functional Requirements Review (FRR) will be conducted prior to system design to ensure all requirements are captured in the Functional Requirements Document and that requirements are stated in a clear, unambiguous and verifiable manner. A Preliminary Design Review (PDR) and/or Critical Design Review (CDR) will be held in order to review, approve, and baseline the system design before actual software coding activities begin. A Test Readiness Review (Tars) shall be conducted prior to the start of independent test & evaluation to ensure that the status of the software and documentation is sufficient to begin System Acceptance Testing (SAT), and when directed by the DHS - User Acceptance Testing (UAT). Release Readiness Reviews (Errs) shall be conducted after SAT, and UAT when directed by DHS, to verify that the software successfully passed independent testing, all required documentation is complete, and outstanding issues have been resolved (i.e. all Scars passed testing, necessary training is complete, no open test problem reports exist, sites are prepared for software release to the production environment, and software distribution methods have been agreed upon).

The Contractor shall comply with the Technical Architecture as specified in the *INS Technology Architecture Overview*, or superceding documents at date of award. The OCIO Architecture Team through the DHS Information Technology Change Request process must approve deviations from the Technical Architecture. The OCIO Architecture Team will conduct design reviews as specified in the SDLC.

7.0 DATA MANAGEMENT – OVERALL TASK

When developing IT applications, the Contractor shall also develop a Data Management Plan which, will include the Application Data Model consisting of clearly documented application data requirements (i.e. application entities, attributes, relationships, and unique identifiers) and the Application Process Model, which documents process requirements (i.e. graphical representation of the processes performed within/by the application) compliant with the DHS Enterprise Model version current at date of award. In addition, the data and process models must follow the logical modeling development standards and specifications documented in the DHS Logical Model Standards version current at date of award. The application Data Management Plan shall be approved and compliant with the enterprise model and to develop the physical database.

8.0 RIGHTS IN DATA - SPECIAL WORKS (FAR 52.227-17)

The clause at FAR 52.227-17 shall be incorporated herein by reference.

9.0 CENTRAL CONTRACTOR REGISTRATION (FAR 52.204-7)

10.0 COMPLIANCE WITH SECTION 508 OF THE REHABILITATION ACT OF 1973, 1998 AMENDMENTS

Electronic and Information Technology products or services delivered by the Contractor shall be in compliance with the Electronic and Information Technology Accessibility Standards (36 CFR 1194).

11.0 SECURITY REQUIREMENTS

11.1 General

DHS has determined that performance of this task order requires that the Contractor, subcontractor(s), vendor(s), etc. (herein known as Contractor), require access to classified National Security Information (herein known as classified information). Classified information is Government information, which requires protection in accordance with Executive Order 12958, Classified National Security Information, and supplementing directives.

The Contractor shall abide by the requirements set forth in the DD Form 254, Contract Security Classification Specification, included in the task order, and the National Industrial Security Program Operating Manual (NISPOM) for the protection of classified information at its cleared facility, if applicable, as directed by the Defense Security Service. If the Contractor has access to classified information at a DHS or other government facility, it will abide by the requirements set by the agency. If the Contractor does not properly follow these procedures, it will result in deductions from monthly invoices.

11.2 Suitability Determinations

DHS shall have and exercise full control over granting denying, withholding or terminating unescorted government facility and/or sensitive government information access for Contractor employees, based upon the results of a background investigation. DHS may, as it deems appropriate, authorize and make a favorable entry on duty (EOD) decision based on preliminary security checks. The favorable EOD decision would allow the employees to commence work temporarily prior to the completion of the full investigation. The granting of a favorable EOD decision shall not be considered as assurance that a full employment suitability authorization will follow as a result thereof. The granting of a favorable EOD decision or a full employment suitability determination shall in no way prevent, preclude, or bar the withdrawal or termination of any such access by DHS, at any time during the term of the task 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 DHS and/or ICE Security Office. Contract employees assigned to the task order not needing access to sensitive DHS information or recurring access to DHS' facilities will not be subject to security suitability screening.

Contract employees awaiting an EOD decision may begin work on the task order provided they do not access sensitive government information or systems. Limited access to government buildings is allowable prior to the EOD decision if a Government employee escorts the Contractor. This limited access is to allow Contractors to attend briefings, non-recurring meetings and begin transition work.

11.3 System Management, Integration, and Administration (SMI) Program Personnel Security Requirements

The Contractor shall provide personnel who will meet the security clearance level for SMI Program.

11.4 Background Investigations

Contract employees (to include applicants, temporaries, part-time and replacement employees) under the task order, needing access to sensitive information, shall undergo a position sensitivity analysis based on the duties each individual will perform on the task 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 30 days before the starting date of the task order or 30 days prior to entry on duty of any employees, whether a replacement, addition, subcontractor employee, or vendor:

1. Standard Form 85P, "Questionnaire for Public Trust Positions"
2. FD Form 258, "Fingerprint Card" (2 copies)
3. Foreign National Relatives or Associates Statement
4. Form DOJ-555, "Disclosure and Authorization Pertaining to Consumer Reports Pursuant to the Fair Credit Reporting Act"
5. Form G-736 – "Pre-Employment Suitability Check" (2 years employment verification)

The Contractor using Form G-736 will provide documentation that previous employers of all new contract employees have been interviewed to ascertain the following information:

a) Verification of employment history (dates, salary, job titles and duties for the most recent 2 years).
b) Reason for leaving employment.
c) Eligibility for re-hires.
d) Name of person contacted.
e) Name of employee doing the interview on behalf of the Contractor.

The Contractor shall conduct and provide the results of the pre-screening employment activity along with a current credit check.

DHS will provide required forms at the time of award of the task order. The Security Office will accept only complete packages. Specific instructions on submission of packages will be provided upon award of the task order.

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

The DHS does not permit the use of Non-U.S. citizens, including Lawful Permanent Residents (LPRs), in the performance of this task order. By accepting this task order, the Contractor agrees to this restriction with respect to all employees utilized directly to perform duties on this task order.

11.5 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 task order.

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

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

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

The ICE Security Office shall be notified of all terminations/ resignations within five days of occurrence. The Contractor shall return any expired DHS issued identification cards and building passes, remote access or strong authentication devices; or those of terminated employees to the COTR. If an identification card or building pass is not available to be returned, a report shall be submitted to the COTR, referencing the pass or card number, name of individual to whom issued, the last known location and disposition of the pass or card.

11.6 Employment Eligibility

The Contractor shall agree that each employee working on this task 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 task order, illegal or undocumented aliens will not be employed by the Contractor, or with this task order. The Contractor shall ensure that this provision is expressly incorporated into any and all subcontracts or subordinate agreements issued in support of this task order.

11.7 Security Management

The Contractor shall appoint a senior official to act as the Corporate Security Officer. The individual will interface with the ICE 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 ICE Security Office shall have the right to inspect the procedures, methods, and facilities utilized by the Contractor in complying with the security requirements under this task order and other DHS or federal security policies, as they are applicable. Should the COTR determine that the Contractor is not complying with the security requirements of this task order, the Contractor will be informed in writing by the contracting officer of the proper action to be taken in order to effect compliance with such requirements.

11.8 Information Technology Security Clearance

When sensitive government information is processed on DHS telecommunications and automated information systems, the Contractor agrees to provide for the administrative control of sensitive data being processed and to adhere to the procedures governing such data as outlined in DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part B.

11.9 Information Technology Security Training Oversight

All Contractor employees using automated systems or processing DHS sensitive data shall be required to receive Information Technology Security Awareness Training as outlined in the Computer Security Act of 1987. Contractor employees may participate in ICE Computer and Telecommunications Security (C&TS sponsored training). However, should they not be available, it is the responsibility of the Contractor to ensure that they have received the appropriate annual awareness training as coordinated with the ICE ~~C&TS~~ OISSM Program Office. All personnel who access DHS information systems will be continually evaluated while performing these duties. Supervisors should be aware of any unusual or inappropriate behavior

by personnel accessing systems. Any unauthorized access, sharing of passwords, or other questionable IT security procedures should be reported to the local DHS Help Desk.

12.0 MINIMUM COMPUTER AND TELECOMMUNICATIONS SECURITY REQUIREMENTS

General

Due to the sensitive nature of DHS information, the Contractor is required to develop and maintain a comprehensive Computer and Telecommunications Security (C&TS) Program to address the integrity, confidentiality, and availability of sensitive but unclassified (SBU) information during collection, storage, transmission, and disposal. The Contractor's security program shall adhere to the requirements set forth in the DHS Management Directive 4300 IT Systems Security Pub Volume 1 Part A and DHS Management Directive 4300 IT Systems Security Pub Volume I Part B and other DHS or ICE guidelines and directives regarding information security requirements. The Contractor shall establish a working relationship with the ICE ~~C&TS~~ OISSM Program Office, headed by the Information Systems Security Program Manager (ISSM).

12.1 C&TS in the Systems Development Life Cycle (SDLC)

C&TS activities in the SDLC are outlined in each current version of the SDLC Manual. The Contractor shall assist the appropriate ICE ISSO with development and completion of all security related activities contained in the SDLC. These activities include development of the following documents:

- *Sensitive System Security Plan (SSSP)*: This is the primary reference that describes system sensitivity, criticality, security controls, policies, and procedures.
- *Contingency Plan (CP)*: This plan describes the steps to be taken to ensure that an automated system or facility can be recovered from service disruptions in the event of emergencies and/or disasters.
- *Security Guide (SG)*: This is a manual that provides users and administrators with detailed requirements on how to operate and maintain a system securely.
- *Risk Assessment (RA)*: This document identifies threats and vulnerabilities, assesses the impacts of the threats, evaluates in-place countermeasures, and identifies additional countermeasures necessary to ensure an acceptable level of security.
- *Security Test and Evaluation (ST&E)*: This document evaluates each security control and countermeasure to verify operation in the manner intended. Test parameters are established based on results of the RA.
- *Certification and Accreditation (C&A)*: This program establishes the extent to which a particular design and implementation of an automated system and the facilities housing that system meet a specified set of security requirements, based on the ST&E of security features and other technical requirements (certification), and the management authorization and approval of a system to process sensitive but unclassified information (accreditation).

12.2 Security Assurances

DHS Management Directives 4300 encourages the use of International Standard 15408, *Common Criteria for Information Technology Security Evaluation*, for evaluating computer systems used for processing SBU information. In addition, the DHS Office of Information Resources Management requires that Contractors adhere to the Department of Defense (DOD) Standard 5200.28-STD, *Trusted Computer System Evaluation Criteria or the equivalent common criteria.* Therefore, the Contractor shall ensure that requirements are allocated in the functional requirements and system design documents to address C2 level of trust, and that these requirements are based on the INS ~~C&TS~~ OISSM Guidance Document 9.0, *Minimum Requirements Document* or the most currently approved DHS directive. C2 systems shall offer the following user-visible features:

- *User Identification and Authentication (I&A)* – I&A is the process of telling a system the identity of a subject (for example, a user) (*I*) and providing that the subject is who it claims to be (*A*). Systems shall be designed so that the identity of each user shall be established prior to authorizing system access, each system user shall have his/her own user ID and password, and each user is authenticated before access is permitted. All privileged users shall have strong authentication, of at least three (3) factors (something you know; something you are; or, something that you have).
- *Discretionary Access Control (DAC)* – DAC is a DHS access policy that restricts access to system objects (for example, files, directories, devices) based on the identity of the users and/or groups to which they belong. All system files shall be protected by a secondary access control measure.
- *Object Reuse* – Object Reuse is the reassignment to a subject (for example, user) of a medium that previously contained an object (for example, file). Systems that use memory to temporarily store user I&A information and any other SBU information shall be cleared before reallocation.
- *Audit* – DHS systems shall provide facilities for transaction auditing, which is the examination of a set of chronological records that provide evidence of system and user activity.

12.3 Data Security

SBU systems shall be protected from unauthorized access, modification, and denial of service. The Contractor shall ensure that all aspects of data security requirements (i.e., confidentiality, integrity, and availability) are included in the functional requirements and system design, and ensure that they meet the minimum requirements as set forth in the legacy INS ~~C&TS~~ OISSM Guidance Document 9.0 or the most current, approved DHS directive at the time of system design or modification. These requirements include:

- *Integrity* – The computer systems used for processing SBU shall have data integrity controls to ensure that data is not modified (intentionally or unintentionally) or repudiated

by either the sender or the receiver of the information. A risk analysis and vulnerability assessment shall be performed to determine what type of data integrity controls (e.g., cyclical redundancy checks, message authentication codes, security hash functions, and digital signatures, etc.) shall be used.

- *Confidentiality* – Controls shall be included to ensure that SBU information collected, stored, and transmitted by the system is protected against compromise. A risk analysis and vulnerability assessment shall be performed to determine if threats to the SBU exist. If it exists, data encryption shall be used to mitigate such threats.
- *Availability* – Controls shall be included to ensure that the system is continuously working and all services are fully available within a timeframe commensurate with the availability needs of the user community and the criticality of the information processed.

12.4 PROGRAM DELIVERABLES

Plans and Schedules

The Contractor shall develop a Task Order Project Plan, containing all resources, activities, and milestones necessary to accomplish work specified in the TORP. Technical activities in the schedule shall be at a level of detail sufficient for the Contractor to manage the task. The Contractor shall develop a new Task Order Project Plan Schedule whenever an Updated Task Order Plan or Revised Task Order Plan is submitted to the DHS for review and approval.

The Contractor shall schedule all activities specified in the TORP including:

a) Management activities
b) Product Assurance activities
c) Design activities
d) Development activities
e) Test activities
f) Deployment activities (each site)
g) Operations and Maintenance activities
h) Reviews
i) Releases
j) Milestones
k) Decision points

The Contractor shall provide an initial schedule and monthly update for each of the SMI Technical Architecture Project.

Progress Reports, Status Reports, and Program Reviews:

12.4.1 Progress Reports:

The Contractor shall prepare monthly progress reports for each project within the SMI Technical

Architecture Project.

Initial reports are due 30 days after task award and every 30 days thereafter until the last month of performance, the final delivery will occur 10 days before the end of the of the final option period and will summarize performance during the period of performance and provide the status of any planned transition activity. The monthly report shall contain the following:

a) Description of work planned
b) Description of work accomplished
c) Analysis of the difference between planned and accomplished
d) Work planned for the following month
e) Open issues

12.4.2 Weekly Status Report

The Contractor shall prepare a weekly status report for the Task Manager for each project. Generally, these reports include the week's accomplishments, any deviations from planned activities; field related issues, other issues, and planned activities for the next period. The weekly reports are for the Task Manager, and may be delivered in a meeting, electronic (e-mail) or in hard copy. Additionally, the DHS Task Manager may request weekly and/or impromptu meetings to discuss status or issues.

12.4.3 Program Reviews

The Contractor shall participate in monthly Program Reviews with the DHS Task Manager or designee to review selected projects. The purpose of this meeting is to ensure that all software modification efforts within the SMI Technical Architecture Project are coordinated, consistent, and not duplicative throughout the Project. Budgets, schedules and other program related issues shall also be addressed when required. The program review is intended to be an informal executive summary of these events, and should require only minimal presentation time.

12.4.4 Cost/Schedule and Earned Value Management System (EVMS) Reporting:

The Contractor shall submit monthly reports to the DHS that must be prepared in sufficient detail to support OMB A-11 reporting requirements at Exhibits 53 and 300. The initial report is due 45 calendar days after task order award and shall cover the first 30 days of task order performance. Subsequent reports will be provided monthly and shall cover the 30-day period that began at the conclusion of the last reported period. At a minimum, the report shall contain the following elements:

Cumulative to date:

- Budgeted cost of work scheduled including fee (award fee estimated at 100%)

- Budgeted cost of work performed including fee (award fee estimate at 100%)
- Actual cost of work performed including fee (award fee estimated at 100%)
- Cost Performance Index and Schedule Performance Index analysis
- Variances between budgeted and actual cost and schedule performance.

- At completion:

  - Budgeted Cost
  - Estimated Cost
  - Variance, if any
  - Cost Performance Index and Schedule Performance Index analysis
  - Variances of more than 10% during any reporting quarter will be discussed in sufficient detail as to identify the underlying causes, corrective action employed and the status of any ongoing corrective activity.

Contractors shall provide the required report in accordance with the formats in Appendix E.

12.4.5 Task Order Funds Status Report

The Contractor shall submit a monthly task order funds status report concurrent with the Cost/Schedule EVMS Report. The status report shall be segregated by government fiscal year and reported on the DHS-ICE - I & SA Funds Status Report Parts A and B at Appendix E. Major subcontractors shall submit Parts C & D of the Funds Status Report. A major subcontract is one that is the lower of either (a) $10 million or (b) $550,000 and more than 10 percent of the task order price.

12.5 SDLC/ECMP AND TECHNOLOGY ARCHITECTURE COMPLIANCE

The Contractor shall provide SDLC/ECMP deliverables required by the appropriate system life cycle phase to the DHS IT Task Manager, Enterprise Library, and Version Manager. Documentation shall be prepared in accordance with the guidelines specified by the SDLC and the approved Tailoring Plan agreed to work pattern; and shall be delivered as specified at **Appendix A** or as incorporated into the approved **project plan**. Additionally, all deliverables shall be in conformance with and implemented within the framework of the prescribed DHS Technology Architecture change process and will be evaluated by DHS within the context of the DHS Enterprise Architecture framework. Deviations from the Approved Work Pattern require an approved RFD by Systems Assurance
Agendas, Minutes, Trip Reports:

The Contractor shall prepare agendas and/or meeting minutes as requested and prepare trip reports for each trip performed under this task order.

12.6 Presentations, Demonstrations and Project Support Materials:

The Contractor shall prepare project presentations, conduct demonstrations, and prepare support materials such as designing system information guides or preparing project displays. It is estimated that at least f two instances of any one of these may be required during a year. Each such instance may encompass a single or multiple projects.

13.0 ACCEPTANCE CRITERIA

13.1 Documentation and Deliverables

Documentation and deliverables will be deemed acceptable if the document adequately covers all required topics; is professionally prepared in terms of format, clarity and readability; and is delivered on time to the designated delivery location. The Contractor shall deliver the correct number of copies and electronic submissions. . All deliverables shall be written and delivered to the task/subtask level and distributed to each different Task Manager accordingly. Specific deliverables related to each Project are outlined in Appendix A and Section 9.0 of this TORP.

13.1.1 Financial Reporting

The Contractor shall deliver two (2) copies in electronic and hardcopy format with a letter of transmittal; one (1) copy of the transmittal letter will be addressed to the contracting officer without attachments.

13.1.2 SDLC deliverables

For all SDLC deliverables, the Contractor shall deliver three (3) copies of each deliverable to the DHS Task Manager in electronic and hard copy format; one (1) copy of the letter of transmittal without attachments shall be delivered to the COTR and the contracting officer.

13.1.3 Task Order Project Plans & Schedules

For all Task Order Project Plans and Schedules, the Contractor shall deliver two (2) copies of each deliverable to the DHS Task Manager in electronic and hard copy format; one (1) copy of the letter of transmittal without attachments shall be delivered to the COTR and the contracting officer.

13.1.4 Progress Reports

The Contractor shall deliver two (2) copies of each monthly Progress Report, one (1) copy shall be addressed to the DHS Task Manager, one (1) copy shall be addressed to the COTR, and the contracting officer shall receive one (1) copy of the transmittal letter without attachments.

13.1.5 Quality Assurance Reports

The Contractor shall deliver two (2) of the Quality Assurance Reports in hard copy and electronic format. Two (2) copies will be provided; one (1) copy shall be addressed to the DHS

Task Manager, one (1) copy will be addressed to the COTR, and a letter of transmittal without attachment will be provided to the contracting officer.

13.1.6 Ad Hoc Deliverables

All other task order deliverables shall be delivered in accordance with instructions specified at the relevant sections of the TORP

13.1.7 Deliverables Summary

Deliverable	Frequency	Copies	Recipients
Financial Reports (EVMS and Funds Status)	Monthly	2	TM (1) copy/ COTR (1) copy / CO (trans ltr.)
SDLC Documentation	As Required	3	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
Task Order Project Plans/Schedules	As Required	2	TM (2) copy/ COTR (trans ltr.), CO (trans ltr.)
Progress Reports	Monthly	2	TM (1) copy/ COTR (1) copy/ CO (trans ltr.)
Quality Assurance Reports	Quarterly	2	TM (1) copy/ COTR (1) copy/ CO (trans ltr)

13.2 Product Acceptance

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

14.0 TASK SPECIFIC DELIVERABLES – TASK A

See Sections 4.4.5 thru 4.4.5.4 for deliverables.

15.0 TASK SPECIFIC DELIVERABLES – TASK B

The following deliverables are representative of the deliverables that ~~will~~ maybe required, as directed by ICE. All deliverables are due 2 calendar weeks after completion of the assignment, unless otherwise directed by ICE.

Engineering Analysis, White Paper, or "Lessons Learned" reports on network problems or poor performance;	Within 2 calendar weeks of completion of assignment
Oral presentation involving questions and answers	Within 2 calendar weeks of completion of assignment unless otherwise directed

Written trip report summarizing issues, findings, accomplishments, and recommendations	Within 2 calendar weeks of completion of assignment unless otherwise directed
Written design specifications with sufficient detail for procurement	As directed
Technology Assessment and Recommendation reports	As required
Systems designs, including engineering diagrams and supporting narratives describing each proposed expansion or enhancement to the International networks, Web Page system, and VTC systems.	As required
Completed as-built information and inventory of all property pertaining to the International network installs/upgrades	Within 2 calendar weeks of completion of assignment unless otherwise directed
Impact Assessment Report—Infrastructure Engineering	As required
Staffing Plan & Organization Plan	As required
White Papers (Resolution of Technical Issues)	As required
Deployment schedules	Two weeks after receiving prioritized list of sites to be deployed.
Pre-Survey Reports	Telephonic with site. Due two weeks prior to conducting site survey.
Site Survey Reports	10 working days after completion of each site survey
Listing of all circuits (Voice and Data) Circuit Order Analysis	Two weeks after effective date of task with monthly updates.
Billing Discrepancy Report Circuit Order Analysis	Monthly
Monthly Progress/Status Report including Description of work planned, Description of work accomplished, Analysis of the difference between planned and accomplished, Work planned for the following month, and Open issues	Monthly
Monthly financial report including planned costs and actual costs incurred, segregated by labor, imaging, storage, shipping, travel.	Monthly

Weekly Task Order Status Report describing the week's accomplishments related to all subtasks including: on-going activities, back-orders, deviations from planned activities, planned activities for the next period, individual team member weekly activities and any issues.	Weekly
IT Infrastructure Support Image Lab Monthly Report addressing the following: Status of configuration and testing of standard and custom images, in accordance with TORP requirement, Develop and Update Standard and Custom Image Configurations; Results of hardware and software compatibility tests, in accordance with TORP requirement; Test Hardware and Software Compatibility Results of new technology test and evaluation, in accordance with TORP requirement; Evaluate and Test New Technologies; Results of analyses of the IT environment, in accordance with TORP requirement, Evaluate and Test New Technologies; Results pertaining to the establishment or revision of technical standards, in accordance with TORP requirement, Assist in Developing Technical Standards	Monthly
Shipping report of all items received into the warehouse and shipped from the warehouse the previous day.	Daily
Staging Facility Standard Operating Procedures (SOPs) including updates to existing Staging Facility SOPs based on USICE approved process and procedural changes	As Needed
Weekly Inventory Report and Receiving Report by program name all items stored within the ICE Staging Facility. The receiving portion of the report shall indicate all items received into the warehouse during the preceding week.	Weekly
Incident Report and CIRP documentation regarding damage or theft at the ICE Staging Facility.	As Needed

Quarterly "Certified" Inventory Report providing the following information: Certified listing of all items stored within the ICE Staging Facility and the report shall indicate all items received in the warehouse during the preceding quarter.	Quarterly
Daily Deployment Status Report including the following information: SLA#, Site Name, Activity, Team Leader, Team Member, Dates, Percentage complete, Accomplishments, Planned Activities, and Issues/Resolutions.	Daily
Deployment Standard Operating Procedures including updates to existing Deployment Standard Operating Procedures based on ICE approved process and procedural changes	As Needed
Deployment Project Plan -	As Directed
Site Survey Report - Documents the results of the site survey that discusses, but is not limited to, the following: the facility, the network topology, hardware and software inventory, user needs, and the identification and follow-up action of any outstanding issues.	As Required
Standard Test Plans for On-Site Installation - Review and update Standard Test Plan procedures for bringing up the installed equipment to its full operational state	As Needed
Test and Analysis Report - Discuss the analysis and results of testing for installation of equipment for each site	As Needed
Close Out Briefing – A briefing that presents the activities, results, and lessons learned from the site installation	As Needed
As-Built Configuration/System Administration Guide - Maintain System Administration Guide (SAG) for each site	As Needed
Inventory Tracking and Warehousing Weekly Report - Provides information on weekly accomplishments, planned activities for the following week, and programmatic issues related to the task.	Weekly
Inventory and Receiving Report - Provides a report on the products received/shipped, quantities received/shipped, storage	Bi-Weekly

location/shipment date, product condition, number of pallet tickets and equipment disposition. Report will also include the manufacturer, serial number, model number, and description of the ADP excess equipment.	

The following deliverables are representative of the deliverables that maybe~~will~~ be required, as directed by ICE. All deliverables are due 2 calendar weeks after completion of the assignment, unless otherwise directed by ICE

Deliverable Number: 1

- Title of Deliverable: Capacity Planning Report
- Description: The ADP Capacity Planning Report shall reflect the workload projections for the JDC-owned mainframes and enterprise UNIX servers at the Justice Data Center (JDC) and full computing resources requirement for the DHS-owned mid-range servers (i.e., UNIX, NT, etc.) at the JDC and at the HQ Operations Center.
- Frequency: Annually
- Dates of Submission: Draft by February 28, 2005; final by March 14, 2005; and reproduced and distributed by March 28, 2005.
- Number of Copies: One electronic copy to the Quality Assurance Manager prior to delivery to the DHS distribution for review and release to the customer.
- One copy of draft and final, via email. Prior to acceptance of the final by the DHS Task Manager, he/she will identify the number of copies required for reproduction and distribution.
- Distribution: One copy of draft and final to the USICE Task Manager. One copy of final to the COTR and the customer Program Office. Reproduced copies will be distributed per direction of the DHS Task Manager.

Deliverable Number: 2

- Title of Deliverable: Monthly Status Report
- Description: The Report shall include, but is not limited to, the following.
  1. Accomplishments
  2. Work-in progress
  3. Planned activities
  4. Staffing changes
  5. Issues of concern
  6. Problems encountered
  7. Proposed/Required solution
- Frequency: Monthly
- Date of Submission: Three (3) workdays after the end of each month. Include projected information for above-listed categories.

- Number of Copies: One electronic copy to the Quality Assurance Manager prior to delivery to the DHS distribution for review and release to the customer. One copy, via email to the DHS Task Manager. One copy of final to the COTR and the customer Program Office.
- Distribution: One copy of draft and final to the DHS Task Manager. One copy of final to the COTR and the customer Program Office.

Deliverable Number: 3

- Title of Deliverable: Weekly Status Report
- Description: The report shall reflect significant work-in progress activities and accomplishments; programmatic problems and issues; next week plans; and travel/training/leave. The Report format shall be in accordance with the Branch weekly reporting format.
- Frequency: Weekly
- Date of Submission: Due by 4 PM each Friday.
- Number of Copies: One electronic copy to the Quality Assurance Manager prior to delivery to the DHS distribution for review and release to the customer. One copy, via email to the DHS Task Manager. One copy of draft and final to the USICE Task Manager. One copy of final to the COTR and the customer Program Office.
- Distribution: One copy of draft and final to the DHS Task Manager. One copy of final to the COTR and the customer Program Office.

Deliverable Number: 4

- Title of Deliverable: Monthly Production Services Staffing Report
- Description: Report shall reflect how each Production Services shift leader function was staffed during the month.
- Frequency: Monthly
- Date of Submission: Due by Noon on the 5th working day after the end of the month.
- Number of Copies: One electronic copy to the Quality Assurance Manager prior to delivery to the DHS distribution for review and release to the customer. One copy, via email to the DHS Task Manager. One copy of draft and final to the USICE Task Manager. One copy of final to the COTR and the customer Program Office.
- Distribution: One copy of draft and final to the USICE Task Manager. One copy of final to the COTR and the customer Program Office.

Deliverable Number: 5

- Title of Deliverable: Monthly Billing and Cpacity Planning/Comsumption Report Description: Report will include reporting on the resource consumption JDC bills for USICE applications systems and hardware (Mainframes, UNIX servers, and small servers, plus storage devices and other supporting infrastructure) supported at the JDC datacenters (DAL and COW). : Report will also include availability (uptime) and

system resource utilization for the major applications run on the JDC mainframes for the USICE customer previously provided in the Monthly Capacity Planning and consumption Report. These applications and systems include: IDMS, CICS, and FOCUS applications, and the mainframe systems supported at the JDC datacenters (DAL and COW).

16.0 TASK SPECIFIC DELIVERABLES – TASK C

The following deliverables are representative of the deliverables that maybe~~will~~ be required, as directed by ICE. All deliverables are due 2 calendar weeks after completion of the assignment, unless otherwise directed by ICE

Deliverable	Frequency	Copies	Recipients
Financial Reports (EVMS and Funds Status)	Monthly	2	TM (1) copy/ COTR (1) copy / CO (trans ltr.)
SDLC/IDLC Documentation	As Required	3	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
Task Order Project Plans/Schedules	As Required	2	TM (2) copy/ COTR (trans ltr.), CO (trans ltr.)
Progress Reports	Monthly	2	TM (1) copy/ COTR (1) copy/ CO (trans ltr.)
SOC Facility and Infrastructure Design Specifications and Plans	As Required	3	TM (2) copy/ COTR (1) copy/ CO (trans ltr)
DMIC Facility and Infrastructure Design Specifications and Plans	As Required	3	TM (2) copies/ COTR (trans ltr.), CO (trans ltr.)
EISA Lab facility and Infrastructure Design specifications and plans	60 days after award	3	
DMIC Operations Procedures	90 days after task award and as required after that	3	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
EISA Lab Operations Procedures	90 days after task award and as	3	

Deliverable	Frequency	Copies	Recipients
	required after that		
C&TS Strategic Plan	120 days after task Award and updated annually thereafter	3	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
C&TS Tactical Plans	180 days after Task Award and updated annually (Fiscal Year) thereafter	3	TM (3) copies/ COTR (trans ltr.), CO (trans ltr.)
C&TS Business Plans	180 days after award and annually (fiscal Year) thereafter	3	
C&TS budget planning and execution tool	60 days after task award and updated as required	3	
ICE Risk Management Plan	120 Days after Task Award and updated annually thereafter	3	
Security Evaluation Reports (SERs) and CO and DAA letters	As required	5	
System Security Plans	As required	5	
Risk Assessments	As required	5	
Security Test and Evaluations (ST&E) Test Plans (pre-production and Operational)	As required	5	
ST&E test reports (pre-production and Operational)	As required	5	

Deliverable	Frequency	Copies	Recipients
Security Guides	As required	5	
Certification and Accreditation (C&A) POA&Ms	As required	5	
C&A/Risk Management Tool analysis	120 days after award	3	
ICE HQ CP and DRPs	As required	3	
ICE OCIO CP and DRPs	As required	3	
Review of ICE System CPs/DRPS	As required	3	
Position and white papers	As required	3	
Role based ~~C&TS~~ OISSM training plan and implementation schedules and requirements	30 days after task award and updated annually (Fiscal Year) there after	3	
ISSO Role based storyboard and supporting design specifications and requirements	60 days after award and updated as required	3	
ISSO training course and support materials	120 days after govt. acceptance of ISSO storyboard	3	
DAA role based training storyboard and supporting design specifications and requirements	30 days after task award	3	
DAA training course and support materials	120 days after Govt. acceptance of DAS storyboard	3	
EISA Lab Product review reports	As required	3	
ICE Security Architecture	180 days after Task	3	

Deliverable	Frequency	Copies	Recipients
	Award and updates annually (fiscal year) thereafter		
ICE IA policy documents	120 days after task award and updated annually (fiscal year) there after	3	
ICE IS procedures, guidelines and other policy related documents	As required	3	
Develop and maintain a model for establishing and supporting ISSOs.	30 days after task award and updated annually (Fiscal year) there after	3	
Position paper on the research and evaluation of smart cards used in combination with other biometric and PKI technologies as a form of electronic identification.	180 days after task award	3	
Develop and document an identification and authentication model/ protocol/strategy for all ICE systems and applications.	270 days after task award	3	
Develop a migration strategy, transition and implementation plan and business case for having one ICE secure Remote Access	210 days after task award		
Develop high-level ICE Security Policy Statement governing PKI and developing policy statements governing the PKI components.	As required		
Define requirements, develop the design, and implement a	As required		

Deliverable	Frequency	Copies	Recipients
prototype for the Cryptographic Services Infrastructure component and also manage and conduct a CSI Pilot.			
Position paper on the research and evaluation of biometrics used in combination with other authentication and PKI technologies as a form of electronic identification.			
Position paper on the research and evaluation of VPN technologies to improve remote access and infrastructure security used in combination with other biometric and PKI technologies.			
ICE Auditing Strategy, business case, implementation plan and other IDLC documentation for the establishment of a comprehensive and centralized ICE Auditing solution that encompasses Windows server and workstation, UNIX, Novell, IBM mainframe; and other major ICE IT infrastructure components	As negotiated with the ICE ISSM and/or task Manager		

17.0 TASK SPECIFIC DELIVERABLES – TASK D

The Contractor shall conduct Task Review Analysis and Coordination (TRAC) meetings (operational/status meetings) monthly or as determined by the Government. The Contractor shall coordinate and participate in all Infrastructure related, OCIO, or DHS meetings as directed by the Task Manager. Additionally, the Contractor shall provide informal, verbal reports regarding task status to the Task Manager upon request.

18.0 MEETING

Meeting	Frequency	Attendance

TRAC (Status) Meeting	Monthly	Task Leader and team members as required
Infrastructure Deployment (Status) meetings	Weekly	Task Leader and team members as required
Infrastructure related meetings	As Required	Task Leader and team members as required
OCIO/ICE/DHS Meetings	As Required	Team members as required

19.0 QUALITY ASSURANCE

The Contractor shall implement a quality assurance program to ensure that all products and services completed under this task order are delivered in accordance with the DHS SDLC Manual. The Contractor shall conduct periodic compliance surveys and report the survey findings on a quarterly basis. The report shall be prepared in Contractor format, the first of which is due three months after task order award.

20.0 PERIOD OF PERFORMANCE

The period of performance for this Task Order is twelve (12) months from date of task order award and includes up to six (6) one-year options to extend performance up to a total of 84 months, or through December 31, 2010, whichever occurs sooner. The last option may not cover a full 12-month period of performance. The Government will provide a 30-day notice of intent before each option is to be exercised.

21.0 TASK ORDER TYPE

This Task Order will include a contract type of Cost Plus Award Fee. The Award Fee Evaluation Plan is provided as Appendix H – Award Fee Evaluation Plan. Cost proposals shall be prepared in accordance with section G.5 of the CIO-SP2i contract. Cost and Award Fee build-ups shall support each individual CLIN. Authorized Base Fee is 0%. See Appendix B, Cost & Pricing Tables. Mapping shall be provided between Mercer Guide Labor Categories and the CIO-SP2i Labor Categories.

22.0 PLACE OF PERFORMANCE

Work on this Task Order will be performed primarily at Contractor's facilities. Frequent travel to DHS offices in the Washington, DC metropolitan area for meetings and briefings will be required. The Contractor's operating facility shall be within 60 minutes travel time to the DHS OCIO Office located 801 I Street NW, Washington DC. Travel to sites outside of the Washington, DC area is required in conjunction with the performance of Task Order project requirements.

23.0 KEY PERSONNEL

A number of billets within the Contractor's organization are expected to significantly affect Program success, and are accordingly designated as key. For this task, the Task Manager shall be designated as Key Personnel and shall be a full-time employee of the Contractor at the time of task award. The Contractor may also designate any other positions to be filled upon award of this Task Order as Key, and such designated personnel shall be required to adhere to the terms and conditions of the Key Personnel provision. Key personnel are expected to serve for the life of the Task, or until replacements with equivalent skills are nominated by the Contractor and accepted by the DHS. In addition to these designations, the Government reserves the right to revise this designation during task order performance, including requiring the identification of additional Key Personnel.

During the first 180 days of contract performance, no key personnel substitutions will be permitted, unless necessitated by compelling reasons including, but not limited to, an individual's illness, death, termination of employment, declining an offer of employment (for those individuals proposed as contingent hires), or maternity leave. In any of these events, the Contractor shall promptly notify the CO and the COTR, and provide the information required herein.

Following this initial 180-day period, the DHS will consider requests for changes in key personnel, if necessary. COTR and CO approval is required prior to any change in key personnel. Requests for key personnel changes shall be submitted in writing at least 30 days in advance of a prospective substitution, and provide a detailed explanation of the circumstances necessitating the proposed substitution, a complete resume of the proposed new personnel, and any other relevant information necessary to evaluate the impact of the prospective substitution on the Program requested by the COTR and CO. The qualifications of proposed substitute key personnel must meet or exceed the qualifications of personnel whom they are proposed to replace. The COTR and CO will generally accept or reject the resume within ten (10) working days.

24.0 GOVERNMENT FURNISHED INFORMATION

A CD with all available documentation relevant to the SMI Technical Architecture Project will be provided to the vendors upon release of the TORP. Upon award (and obtaining required security clearance), the successful Contractor will be provided access to the Enterprise Library at 1101 Vermont Avenue, NW, Suite 220, Washington, DC, 20005. This is the central repository for all DHS IT Systems documentation.

25.0 GOVERNMENT FURNISHED EQUIPMENT/PROPERTY

Government furnished equipment/property relative to project requirements are identified at Appendix C and will be transitioned to the Contractor after Task Order Award. The Contractor

shall manage, maintain, and control all Government Furnished Equipment / Property in support of this Task Order in accordance with FAR 52.245-5.

In accordance with FAR 45.505-14, the Contractor shall prepare and submit an annual report of Government property for which the Contractor is accountable as of December 31 of the previous year. The Contractor shall submit the report to the cognizant administrative contracting officer no later than January 31st of each year.

26.0 OTHER DIRECT COSTS (ODCS)

The Contractor shall propose anticipated ODCs with appropriate justification and explanation in its technical and cost proposals. Once accepted those anticipated costs would be included in the total estimated cost ceiling applied to the awarded task order. In any case, all ODC expenditures shall be pre-approved by the Government in accordance with the following guidance:

- The DHS-ICE Task Manager will approve individual ODC requests totaling **$2,500** or less and all-domestic travel. This approval authority specifically **excludes** the purchase of personal computers (PCs), laptops, cell phones, pagers, handheld computers, cameras, and video equipment, in addition to computer systems/workstations, software and training which can only be approved by the COTR.
- The COTR will approve all international travel based on the recommendation of the DHS -ICE Task Manager. Task Managers will review requirements, i.e. purpose of the trip, destination, number of travelers, and the duration of each trip.
- The COTR will, with the recommendation of the DHS Task Manager, approve all requests for payment of Contractor training cost. The DHS-ICE will only pay for training costs associated with the training of Contractor personnel necessary to support DHS unique applications/requirements. The DHS-ICE expects that all Contractor personnel will be properly trained and maintain proficiency in their field of expertise at no additional cost to the Government. Therefore the Government will not pay for training courses or seminar that Contractor personnel would normally attend to remain proficient or current in their fields of expertise. Costs associated with such training will be the sole responsibility of the Contractor.

27.0 INVOICE SUBMISSION

The Contractor shall prepare invoices in accordance with SECTION G.2 of the NIH CIO-SP2*i* contract, entitled PREPARATION OF VOUCHERS and submit them directly to the DHS Accountable Management Official (AMO). (Note: The AMO is also the DHS Procuring Contracting Officer (PCO) and Administrative Contracting Officer (ACO).)

A. The cognizant audit office:

Defense Contract Audit Agency

Mid-Atlantic Region
Alexandria Branch Office
8725 John Kingman Road, Suite 2135
Fort Belvoir, VA 22060-6228

B. Accountable Management Official:

Robert H. Richards
HQ Procurement Division
801 I Street, N.W., Suite 700
Washington, DC 20536

C. Customer Finance Office:

[DO NOT SUBMT INVOICES TO THE FINANCE DEPARTMENT]

ICE Finance Office
800 K Street, NW
Room 1000
Washington DC 20536

D. Contracting Officer Technical Representative address:

Sheilita Williams
Office of Information Resources Management
801 I Street, N.W., Suite 710
Washington, DC 20536

In addition to the requirements listed above, the Contractor shall provide the following documentation with each submitted invoice:

The following information for each CLIN for each person being billed:

- Labor category
- Name of person and rate
- The period of performance that shows the start date (Month/Day/Year) the end date (Month/Day/Year) and, the associated number of hours being billed.
- Total Cost per labor category.
- Other Direct Costs (ODCs)
- ODC Details: The cost reimbursable invoice for a billing period shall include the following information by CLIN:
- Amount and description of each ODC including associated date or dates
- Total amount for all ODCs
- Cumulative amount of ODCs
- Total reimbursable costs

28.0 AVAILABILITY OF FUNDS

Funds are available for this task order or will become available prior to award.

29.0 LIMITATION OF FUNDS

The Government will incrementally fund cost reimbursable line items; FAR 52.232-22 (April 1984) applies.

30.0 TRANSITION

The Contractor shall be responsible for the transition of all technical activities identified in this task. The Contractor shall complete the technical transition within 60 days after task order 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 Government Furnished Equipment/Property (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, if any.
- Coordinating the body of work with the current Contractor and turnover of tasking, staffing, etc.

The Contractor's transition plan shall be approved by the DHS and shall contain a milestone schedule of events and system turnovers. The transition plan shall transition systems with no disruption in operational services. The Contractor shall provide the transition plan 7 days after task order award. To ensure the necessary continuity of services and to maintain the current level of support, the DHS will retain services of the incumbent Contractor for the transition period, if required.

At the completion of the period of performance of this task order, the Contractor shall fully support the transition of SMI Technical Architecture requirements to the successor vendor. Activities 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 task order including exercised options, the contracting officer will issue a modification to authorize and fund the transition activity of the outgoing Contractor.

31.0 FAR CLAUSES INSERTED BY REFERENCE

The following clauses are hereby inserted by reference and have the same force and effect as if they were inserted full text into awarder's contract:

31.1 52.204-7 Central Contractor Registration (OCT 2003)

31.2 52.232-33 Payment by Electronic Funds Transfer – Central Contractor Registration (OCT 2003)

32.0 PACKAGING, PACKING, AND SHIPPING

The Contractor shall ensure that all items are preserved, packaged, packed and marked in accordance with best commercial practices to meet the packing requirements of the carrier and to ensure safe and timely delivery at the intended destination.

All data and correspondence submitted shall reference:

A. The CIO-SP2*i* Task Order Authorization Number
B. The NITAAC Tracking Number
C. The Government end user agency
D. The name of the COTR

Containers shall be clearly marked:

A. Name of Contractor
B. The CIO-SP2*i* Task Order Authorization Number
C. The NITAAC Tracking Number
D. Description of items contained therein
E. Consignee(s) name and address