

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 9 of 82
--	----------------------------	---	--------------

Section 2 – Statement of Work
Office of Historical Trust Accounting (OHTA) – IT Support Services

2.0 Introduction

This statement of work describes the services required to support the OHTA information management systems and hardware/software platform.

2.1 Background

With the enactment of the General Allotment Act of 1887, the United States Government was directed to serve as the trustee for tribal land, resources, and monetary assets. The Department of the Interior (DOI) has managed this fiduciary responsibility by administering Individual Indian Money (IIM) and Tribal trust funds for Native Americans and Alaska Natives. Historically, DOI's Bureau of Indian Affairs (BIA) and Office of the Special Trustee (OST) have managed these funds, including more than 1,400 Tribal accounts and 258,000 IIM accounts, with total cash assets greater than \$3 Billion. In 1996, five plaintiffs filed a class action lawsuit, *Cobell v. Babbitt* (currently referred to as *Cobell v. Salazar*), alleging that the United States Government had mismanaged these trust assets throughout its tenure as trustee. The U.S. District Court, and subsequently, the D.C. Circuit Court of Appeals, ruled in the plaintiffs favor and directed the DOI to conduct an historical trust accounting as required by law.

The Office of Historical Trust Accounting (OHTA) was established by Secretarial Order in July 2001 to plan, organize, direct, and executes the historical accounting of IIM trust accounts. The Secretarial Order has been amended twice to expand OHTA's role to include accounting reviews leading to the distribution of funds from Special Deposit Accounts and a review of Tribal Trust accounts.

2.2 Objective

The coordination of work and integration of information and information technology (IT) to support execution of the historical accounting effort is of critical importance to OHTA's success. Given the vast scope and complex nature of the work that must be accomplished, OHTA requires a multi-disciplinary, experienced contractor to provide IT and project Development and integration support. The objective of this statement of work (SOW) is to define the on-going and future tasks that the contractor will perform to meet OHTA's requirements. This SOW outlines the tasks that will be accomplished as well as provides a high-level overview of the deliverables that will be developed and an approximate timeline for delivery.

2.3 Scope

The scope of this contract is to provide a variety of IT system development, operational and maintenance (O&M) support services, and information security to OHTA. The contractor shall provide services in the areas of Project Management, Operation and Maintenance (O&M) Services, Hosting/Housing Environment Support, System(s) Development, Database Support, Internet and Intranet Publishing and Publishing Management, Configuration Management, End-User Support, Security Management, Vulnerability and Patch Management, and Contingency Planning and Management support. The Contractor will use a comprehensive, overarching project management approach to ensure that costs are controlled, schedules are met, return on investment (ROI) is maximized, and business/program objectives are attained.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 10 of 82
--	----------------------------	---	---------------

2.4 General Requirements

2.4.1 Information Protection and Nondisclosure

2.4.1.1 All Government-provided data received, processed, evaluated, loaded, and/or created as a result of the contract shall remain the sole property of the Government unless specific exception is granted by the Contracting Officer (CO). The Government owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as a result of the contract provided under FAR 52.227-14 and 52.227-17 as incorporated into this contract. Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.

2.4.1.2 Any and all information made available to the Contractor by the Government for the performance or administration of this contract shall be used for those purposes and shall not be used in any other way without the written agreement of the CO and the contracting officer's appointed representative (COR or COTR).

2.4.1.3 All information that is government owned in accordance with subparagraph 2.4.1.1, above, is to be returned or destroyed upon contractor receipt of instructions from the OHTA Chief Information Officer (OHTA CIO), instructions that the contractor will immediately comply with. Upon expiration of the contract and/or tasks under it, all documents released and any material containing data from such documents shall be automatically returned to the COR for final disposition. Exception: If the Contractor receives a data disposition request, and sees a need to keep any information that is to be deleted or returned, the Contractor may request and will obtain an advance written approval from the OHTA CIO to retain any Government-furnished information and/or data. Requests must establish and justify why and for what purposes the material is directly relevant and is needed for future contract-related use as part of supporting material to work papers/working papers/work in progress, etc. being created by the contractor as part of a deliverable. Sweeping Data from Devices: The Contractor shall comply with requests from the government to exercise oversight over the contractor's use of and compliance with Government-provided sanitization instructions and software applications to be employed to remove data from all systems and storage media to ensure that residual magnetic, optical, electrical, or other representation of data that has been deleted and is not recoverable.

2.4.1.4 The Contractor shall ensure the return to the COR all such agency badges, card keys and all other Government furnished equipment (GFE) and Government Furnished Information (GFI) upon completion of performance or when personnel depart permanently or for an extended period of time (more than 30 days). The Contractor shall report all incidents of lost or stolen badges, card keys, or GFE/GFI to the COR and the OHTA CIO no later than one (1) hour after realization or suspicion that such loss has occurred.

2.4.1.5 The Contractor shall report to the COR all contacts with entities individuals, and counsel/representatives (including foreign entities and foreign nationals not associated with the contractor and/or this contract engagement), who seek to obtain any access to OHTA information. The Contractor shall report all violation(s) of contract provisions, laws, executive orders, regulations, and/or policies to the contracting officer. The Contractor shall report any information

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 11 of 82
--	----------------------------	---	---------------

raising a doubt as to whether an individuals' eligibility for continued employment or access to sensitive information is consistent with the best interests of National Security and/or the Public Trust. Unsanctioned, negligent, or willful inappropriate action on the part of the Contractor (or its employees, subcontractors, or subcontractor's employees) may result in termination of the contract or removal of any Contractor (or subcontractor) employee from OHTA buildings and/or facilities. These actions include, but are not limited to, exploration of a sensitive system and/or information, introduction of unauthorized and/or malicious software, failure to follow prescribed access control policies and/or security procedures, or other established security requirements.

- 2.4.1.6** Media sanitization and information disposition activity is usually most intense during contract/task termination. However, throughout the life of an information system, many types of media, containing data, will be transferred outside the positive control of the Contractor. This activity may be for maintenance reasons, system upgrades, or during a configuration update. Before any media are sanitized, the Contractor shall consult with the OHTA CIO and COR. This consultation is to ensure compliance with record retention regulations and requirements in the Federal Records Act. In addition, this will also ensure that historical information is captured and maintained where required by OHTA business needs. The Contractor must provide written confirmation of the sanitization and disposition of the storage media to the OHTA CIO via the COR immediately upon completion of the media sanitization.
- 2.4.1.7** The OHTA CIO, as the information custodian, is responsible for ensuring that the Contractor follows the sanitization guidelines and requirements.
- 2.4.1.8** The Contractor shall protect the information from unauthorized release to the public, or to unauthorized persons, organizations, or subcontractors. All DOI and /or OHTA Information has been deemed sensitive and will be secured in accordance with instructions provided by the Government. All these provisions shall also apply to all subcontractors working on behalf of the contract.
- 2.4.1.9** The Contractor or subcontractor shall not disclose or release any sensitive, or otherwise protected information, regardless of medium (e.g., film, tape, document, electronic), pertaining to any part of this contract or any OHTA program or activity, to any activity or individuals of the Contractor's or subcontractor's organization that has not undergone an applicable suitability and/or background investigation commensurate with the contract specifications.
- 2.4.1.10** Contractor employees, agents, advisors, consultants, contractors, and/or subcontractors who will have access to DOI information or will develop custom applications must (1) be notified that such information is sensitive, protected and/ or confidential and will be received in confidence by employee agents, advisors, consultants, contractors, and/or subcontractors as set forth in this contract, (2) must sign a Confidentiality/Non-Disclosure Agreement indicating that he or she has read the Non-Disclosure Agreement and understands that such Agreement governs the handling of sensitive, protected and/or confidential information, prior to gaining access. Copies of all Non-Disclosure Agreements will be maintained in the OHTA contract file and with the OHTA physical security office.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 12 of 82
--	-----------------------------------	--	---------------

2.4.1.11 Unless ordered by valid subpoena or other appropriate court order the Contractor shall not release any sensitive, or otherwise protected information, regardless of medium (e.g., film, tape, document, electronic), pertaining to any part of this contract or any OHTA program or activity, unless the CO or COTR has given prior written approval.

2.4.1.12 Requests for approval of information disclosure shall identify the specific information to be released, the name and address/email/telephone number of the requestor seeking the information, the medium to be used, and the purpose for the release. The Contractor shall submit its request to the COR at least 10 business days before the proposed date for release. If the COR cannot respond within 10 days, the release shall be delayed until approval is received from the COR.

2.4.1.13 The Contractor shall provide adequate physical protection to information technology to preclude access by any individual or entity not authorized by the Government. The Contractor shall maintain, and furnish upon request of the CO, COR or OHTA CIO records of the names of individuals who have access to sensitive material in its custody. All questions regarding classification, access and control shall be referred to the CO, COR, or OHTA CIO.

2.4.1.14 Contractor shall report all incidents involving suspected or known breach if personally identifiable information (PII) in electronic or physical form and should not distinguish between suspected and confirmed breaches to the DOI-OHTA CIO and COR within one hour of discovery. The Contractor shall immediately notify (within 1 hour) the COR and OHTA CIO in writing in the event that the Contractor determines or has reason to suspect a non-PII breach of security requirements.

2.4.1.15 The contractor must report computer security incidents affecting DOI data or systems in accordance with the DOI Computer Incident Response Guide.

2.4.2 Handling of Protected Information

2.4.2.1 Non-Federal employees (i.e., Contractor’s employees, agents, advisors, consultants, contractors, and/or subcontractors) will be granted access to sensitive information on a need-to-know basis only. Information supplied as Government-furnished materials to a non-Federal employee, including anyone who produces new, original work, is to be returned upon completion of the authorized work to the COR, no later than 30 calendar days of contract closure. The Contractor agrees that sensitive information will be handled as follows.

2.4.2.2 Sensitive information (which includes PII and Indian Trust data) shall be properly handled, stored and protected from the risk and magnitude of loss or harm that could result from inadvertent or deliberate disclosure, alteration or destruction. The DOI Information Technology Security Policy Handbook, Version 3.1, dated March 17, 2008, defines the security requirements for Sensitive but Unclassified (SBU) and For Official Use Only (FOUO) information.

“Sensitive Information” is defined as any information, the loss, misuse, or unauthorized access to or modification of which could adversely affect the national interest or the conduct of federal

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 13 of 82
--	-----------------------------------	--	---------------

programs, or the privacy to which individuals are entitled under Section 552a of Title 5, United States Code (the Privacy Act), but which has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept secret in the interest of national defense or foreign policy.

“Personally Identifiable Information”(PII) means any information about an individual maintained by an agency, including, but not limited to, education, financial transactions, medical history, and criminal or employment history and information which can be used to distinguish or trace an individual's identity, such as their name, social security number, date and place of birth, mother’s maiden name, biometric records, etc., including any other personal information which is linked or linkable to an individual.

“*For Official Use Only (FOUO)*” is a document designation that is used to identify information or material which, although unclassified, may not be appropriate for public release. There is no Federal Government standard governing use of the FOUO designation. FOUO information is unclassified sensitive information that is or may be exempt from public release under the FOIA. During non-business hours (generally 8:15 pm to 5:30 am local time) sensitive information must be secured within a locked office or suite, or secured in a locked container.

- 2.4.2.3 Sensitive information may be sent via the U.S. Postal Service or commercial delivery or messenger service, provided it is by “accountable mail” (i.e. registered, trackable-express mail, insured, etc.) and packaged in a way that does not disclose its contents. The Contractor shall encrypt all data on removable media, and portable/mobile devices when in transit.
- 2.4.2.4 The Contractor shall NOT provide access to information to employees or subcontract employees, until a Non-Disclosure Agreement (NDA) is signed (Sec 3, Attachment 2) and on file with the OHTA Physical Security Officer, and written access clearance approval is provided by the COR and the OHTA Physical Security Officer.
- 2.4.2.5 The Contractor shall encrypt all data on removable media, portable/mobile devices and remote workstations which carry OHTA data unless the data are determined to be non-sensitive in accordance with the procedure in the DOI Information Technology Security Policy Handbook. The determination of non-sensitive data will be provided to the Contractor in writing by the COR and approval by the OHTA Delegated Approving Authority (DAA). The Contractor will use only OHTA provided encryption software and hardware or Government approved encryption software and hardware. In the case that the government supplies the software, the provisions of FAR clause 52.245.4, Government Furnished Equipment (GFE), shall apply. If the Contractor is instructed to acquire and use specific government designated software from a third party, prior to purchasing the software, the contractor shall obtain quotes from various sources and supply them to the CO, with recommendation as to which source the vendor finds most advantageous considering price and availability. The CO may decide to issue a Government order to the supplier and deliver the software to the Contractor as a government furnished equipment. The Contractor may bill the Government for the cost of the software plus a reasonable charge for administering the purchase, if the CO instructs the contractor to obtain the software using its own resources. Upon reimbursement of the contractor by the government, the software shall become

	Document No. DI1PD18655	Document Title OHTA- IT Support Services	Page 14 of 82
--	----------------------------	---	---------------

government property that the Contractor shall relinquish to the COR at OHTA at the end of the order period of performance or whenever the equipment is no longer needed.

2.5 Physical Security - General Procedural Security Requirements

2.5.1 The Contractor's employees, agents, advisors, consultants, contractors, and/or subcontractors governed by this contract may need to access sensitive information and/or access to designated restricted areas. The Contractor is responsible for providing security briefings regarding, and ensuring compliance by its employees, agents, advisors, consultants, contractors, and/or subcontractors with, any applicable security procedures of the Government installation (facility) or non-government facility, where sensitive work may be performed under this contract. This briefing shall include topics such as the safekeeping, wearing, and visibility of a Contractor-provided picture name badge or any special agency security and/or identification badges.

The contractor shall ensure the return to the COR all such agency badges, card keys and all other Government Furnished Equipment (GFE) and Government Furnished Information (GFI) upon completion of performance or when personnel depart permanently or for an extended period of time (more than 30 days). The contractor shall report to the COR all contacts with entities individuals, and counsel/representatives (including foreign entities and foreign nationals not associated with the contractor and /or this contract engagement) who seek to obtain any access to OHTA information. The Contractor shall report all violation(s) of contract provisions, laws, executive orders, regulations, and/or polices to the contracting officer. The Contractor shall report any information raising a doubt as to whether an individuals' eligibility for continued employment or access to sensitive information is consistent with the best interests of National Security and/or the Public Trust. Unsanctioned, negligent, or willful inappropriate action on the part of the Contractor (or its employees, subcontractors, or subcontractor's employees) may result in termination of the contract or removal of any Contractor (or subcontractor) employee from OHTA buildings and/or facilities. These actions include, but are not limited to, exploration of a sensitive system and/or information, introduction of unauthorized and/or malicious software, failure to follow prescribed access control policies and/or security procedures, or other established security requirements.

2.6 Administration

The contractor shall designate a single representative who shall represent the contractor. Only that designated individual will accept instructions and authorizations to proceed with production of deliverables when delivered by the contracting officer's appointed representative (COR or COTR), acting within the authority of the COTR's appointment letter.

2.7 Approval of Travel, other than local commuting

Contractor shall obtain COTR's advance written approval of travel costs which are to be billed to the Government. No reimbursement is authorized for local commuting or local area travel. Costs for travel undertaken without prior COTR approval will not be reimbursed.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 15 of 82
--	-----------------------------------	--	---------------

2.8 Contractor Location.

All Software development shall be performed within the United States and outsourced operations shall be located in the United States.

2.9 Use of Personally-Owned/ Contractor-Owned Equipment/and Government-Owned Equipment & Information

2.9.1 Use of Personally-Owned Equipment

The Department of the Interior prohibits the installation and use of personally-owned equipment in DOI owned or leased buildings. Personal cell phones may be used in facilities that allow personal cell phones. However, the Department prohibits the use of any personally-owned information system from directly or remotely accessing Interior's network or network resources, to include remote access of any Interior e-mail system with an Internet-accessible interface. The Department also prohibits the use of any personally-owned information system from accessing, processing, storing, and/or transmitting any Personally Identifiable Information (PII) or any other sensitive agency information. Violation of this provision may result in immediate contract termination.

2.9.2 Requirements for the Use of Contractor-Owned Equipment

All contractor-owned equipment and/or software used to connect to DOI systems or to develop applications for DOI must be certified and accredited in accordance with DOI policy and standards. The OHTA Chief Information Officer (CIO) shall approve, in writing, the use of contractor-owned equipment and/or software, citing no adverse effects on DOI IT resource(s) or the network.

2.9.3 Government Furnished Equipment (GFE)/ Government Furnished Information (GFI)

The OHTA shall provide the following hardware and software:

- OHTA will provide workstations, laptops, and any essential accessories along with OHTA network access to all members under this contract.
- OHTA will provide the development, test, pre-production, production and any other server based environment necessary to accomplish the statement of work.

2.10 Task Requirements

2.10.1 Contract-wide IT Project Management

2.10.2 Project Management Support

The Contractor shall provide an overarching, contract-wide IT project management capability for all projects and special tasks issued under the contract. The Contractor shall provide program management planning, work breakdown structure (WBS) development and tracking, performance monitoring, risk management, and earned value management. Provide accurate and timely project status reports. Manage the sum of all active and planned projects as a portfolio. Determine and communicate the impact of a change on one project to all other active or planned projects. Manage multiple projects simultaneously with a defined resource pool. Coordinate with and oversee work performed by third-party organizations. Manage critical paths, coordinate key

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 16 of 82
--	----------------------------	---	---------------

integration points, and develop contingencies to deal with the risk and uncertainty inherent in IT projects. Provide ad hoc organizational reporting support to include, but not be limited to, the gathering and compilation of information for Office of Management and Budget submissions and other Departmental or Government-wide calls for information, and the gathering and assembling of information for OHTA weekly report submission.

2.10.3 Work Breakdown Structure (WBS)

The contractor shall develop a Work Breakdown Structure (WBS) and WBS dictionary to at least the third level of breakdown and detail (work packages). Work packages are the level at which the project manager has to monitor all project work.

2.11 Risk Management

2.11.1 For each task, as they are planned during the life of the contract, the contractor shall develop and maintain (update) a risk management plan that will be used for risk assessment (likelihood and consequence), mitigation planning, and monitoring. Risk monitoring shall track changes in risk assessment, status of mitigation actions, and emerging risk impacts. The contractor shall use the government furnished risk management process and plan as the baseline document.

2.11.2 Project lead/Risk Manager specific responsibilities include the following activities:

- Maintain the Risk Management Plan.
- Plan and coordinate risk management meetings.
- Plan and manage risk management training.
- Generate risk reports for risk meetings and ad-hoc requests.
- Maintain and monitor data in the risk management tool.
- Establish initial priority, owner, and target due date.
- Monitor the status of risk mitigation.
- Communicate status to risk originators and risk owners.
- Escalate communication if expected mitigation action deadlines are not met.
- Execute the risk closure process.
- Work with project team leads members to facilitate risk mitigation.

2.11.3 Quality Control Plan (QCP)

The Contractor shall develop and implement a Quality Control Plan (QCP) to ensure all deliverables provided and services performed under the contract are accurate, complete and free of errors. The QCP shall address both technical and administrative deliverables and services. *The Government will not serve in the quality control function for the contractor.*

2.11.4 Technical Review Meetings

The Contractor shall hold technical review meetings government and contractor management/team leads and end users to support the management and development of software version releases. The Review shall consist of but not be limited to:

- System Requirements review (SRR)
- System Design/Definition/Functional Review (SDR/SFR)
- Software Specification Review (SSR)

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 17 of 82
--	----------------------------	---	---------------

- Preliminary Design Review (PDR)
- Critical Design Review (CDR)
- Test Readiness Review (TRR)
- Production Readiness Review (PRR)

2.11.5 Performance Monitoring, Optimization and System Maintenance –

The Contractor shall conduct semi-annual performance measurement and evaluation activities that may lead to re-engineering and/or optimization of existing websites and applications to improve productivity, system performance, network throughput, changing functional and technical requirements or any other constraints identified by the Government personnel.

2.12 Operation and Maintenance (O&M) Services

2.12.1 Infrastructure Support Management

Managing OHTA’s infrastructure servers and clients require the contractor to be responsible for managing the servers and standardized desktop workstations attached to the network. Management of all systems shall encompass client/server operations and maintenance, configuration management, installations, implementation, performance and capacity planning, office automation, and collaborative tools.

2.12.2 System Sustainment

2.12.2.1 The contractor shall maintain the day to day system operating environment, and keep the systems in operating condition, consistent with requirements. This includes: sustainment of reports/queries, utilities and menus.

2.12.2.2 The Contractor shall respond to high priority trouble calls and resolve application problems immediately.

2.12.2.3 The Contractor shall anticipate and identify problem areas and solutions to avoid or recover delays.

2.12.2.4 The Contractor shall adjust and respond to application emergencies immediately.

2.12.3 Systems Administration.

2.12.3.1 This includes installation of new or modified software; managing accounts, network rights, and access to systems and equipment; monitoring the performance, capacity, serviceability, and recoverability of installed systems; implementing security procedures and tools; resolving hardware/software interface and interoperability problems; and maintaining systems configuration and inventory.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 18 of 82
--	----------------------------	---	---------------

2.12.4 Systems Management.

2.12.4.1 The Contractor shall maintain and support all servers listed in Attachment (1). This includes monitoring and analyzing system activity and performance and making recommendations to the Government to make changes to proactively avoid outages or to make improvements to prevent degraded performance. It also includes performing standard system upgrades (e.g., install patches or upgrade software release) on a routine or ad hoc basis based upon the frequency of vendor software releases, as pre-approved by the Government CCB process. This activity also may require coordinating on-site servicing by a vendor. The Contractor shall maintain and support all workstations of the type listed in Attachment (2). The Contractor shall be responsible for installing and configuring the workstations. The Contractor shall install/maintain Antivirus updates.

2.12.4.2 The Contractor shall coordinate routine software or hardware preventive maintenance and backup schedules with the Government and other vendors.

2.12.5 Information System Backup

2.12.5.1 The Contractor shall conduct backups of user-level and system-level information (including system state information) contained in all information systems (differential daily and full weekly) and protects backup information at the storage location. This is to include the archiving of critical data sets to media, such as tape, optical disc and/or disk cartridges.

2.12.5.2 The Contractor shall test backup information at least annually to verify media reliability and information integrity.

2.12.5.3 The Contractor shall selectively use backup information in the restoration of information system functions as part of contingency plan testing.

2.12.5.4 The Contractor shall store backup copies of the operating system and other critical information system software at a separate facility or in a fire-rated container that is not collocated with the operational software.

2.12.5.5 The Contractor shall protect system backup information from unauthorized modification.

2.12.6 Information System Recovery and Reconstitution

- 1) The Contractor shall restore systems from backup or restore systems after system crashes.
- 2) The Contractor shall employ mechanisms with supporting procedures to allow all information systems to be recovered and reconstituted to a known secure state after a disruption or failure.
- 3) The Contractor shall include a full recovery and reconstitution of information systems as part of annual contingency plan testing.

2.12.7 Maintenance Support

The contractor shall provide technical services to support on-site maintenance (Scheduled and Remedial/ Malfunction Maintenance). This includes routine configuration management issues,

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 19 of 82
--	----------------------------	---	---------------

critical issues such as recovery from catastrophic system failures, and development/integration of new imagery functions as required.

2.12.7.1 Controlled Maintenance

The Contractor shall schedule, perform, document, and review records of routine preventative and regular maintenance (including repairs) on the components of all information systems in accordance with manufacturer or vendor specifications and/or OHTA requirements. The Contractor shall maintain maintenance records for information systems that include:

- the date and time of maintenance;
- name of the individual performing the maintenance;
- name of escort, if necessary;
- a description of the maintenance performed; and
- a list of equipment removed or replaced (including identification numbers, if applicable).

2.12.7.2 Scheduled Maintenance

Scheduled Maintenance shall be at a time other than during Government's working hours unless otherwise specified by the Government. The contractor shall specify the number of hours required for preventive maintenance of systems identified in (Attachment 1). The contractor shall also specify in writing the frequency and duration of the preventive maintenance. The Government shall by mutual agreement, specify the schedule for the performance of scheduled preventive maintenance.

2.12.7.3 After-Hours Maintenance Support

The Contractor shall respond to after-hours calls from the Government designated POC. The Contractor's personnel shall be available via telephone and/or pager to respond to critical system deficiencies or other operational contract-related issues that may arise such as recovery from system failures. The support personnel shall provide via telephone instruction/guidance over the telephone or by remotely accessing defective machines. The contractor is to have a support team in place to travel to the sites of problems in the event that telephonic or remote assistance fails to remedy an issue during hours other than normal duty hours.

2.12.8 Account Management.

The Contractor shall create and delete accounts for network access as well as for all systems managed, based on the system request access form. The Contractor shall create an account within 8 working hours from the receipt of the request. When requests to create an account exceed 10 in one working day, the Contractor shall create the accounts within 16 working hours from the receipt of the requests. All account creation requests must come through the Help Desk. The Contractor shall lock unused accounts after 90 days and delete unused accounts after 180 days. The Contractor may unlock the account after receiving authorization from user's supervisor or Government personnel with appropriate authorization privileges. The Contractor shall deliver a quarterly report detailing list of accounts that required unlocking including who granted the unlocking.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 20 of 82
--	----------------------------	---	---------------

2.12.9 Software Installation

For GOTS/COTS packages assigned to the Contractor for installation/update, the Contractor shall provide the Program Manager with a Change Request (CR). Upon approval of the CR, the Contractor shall install or update the GOTS/COTS software, test the software together with the originator of the ECP/SPR, and produce a test report from the government Program Manager.

2.12.10 Production Support

The Contractor shall provide on-going support and maintenance of the existing production environment. Detailed activities related to production support are listed below:

- Updating the production BIOS and firmware server software to vendor recommended and supported versions
- Testing and deploying to production the latest relevant Microsoft updates and virus definitions
- Loading images to production servers
- Performing nightly database and working paper drives backups
- Maintaining and monitoring the storage available on all servers
- Providing on-going user support

2.12.11.1 Trusted Facility Manual (TFM)

The Contractors system developers shall create and maintain a Trusted Facility Manual (TFM). Configuration standards and management procedures shall be used to control usability, efficiency, and security of the overall server environment and shall be kept in TFM.

2.12.12 Telecommunications Administration, Support and Maintenance

Provide support for telecommunications requirements to include cable installations, testing of fault isolation circuits and perform problem diagnostics and analysis. Work with the DOI building operations and telecom organizations to address backbone, WAN, hardware, protocol issues. Manage IP addresses for the Technical Services Group.

2.12.12.1 The Contractor shall provide management and technical support for OHTA's telecommunications services including teleconferencing, voice, voice mail, video teleconferencing, cable television, and conference room audio/visual systems.

2.12.12.2 The Contractor's responsibilities shall include, but are not limited to, providing the following telecommunications services:

- Provide management of OHTA's telecommunications services during standard hours of operation to ensure requests for services, service changes, maintenance, and service disconnect are addressed.
- Provide moves, additions, and changes of phone service at the PBX, communication closet, internal circuit and handset levels.
- Provide problem resolution, including, but not limited to, identifying problems, troubleshooting, coordinating repair of telecommunications equipment, site visits to

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 21 of 82
--	----------------------------	---	---------------

perform maintenance by external providers, the return of equipment to vendor for repair and tracking of equipment being repaired.

- Work with commercial vendors or other service providers to resolve installation, performance and service disconnect issues in a timely manner.
- Manage and maintain OHTA's voice messaging systems, including, but not limited to, system configuration, mailbox configuration, add/delete/change voice mailbox configurations, and maintain documentation of system/mailbox configurations. Regularly audit voice mail accounts to ensure voice mail assignments are current, accurate and comply with federal regulations.
- Design, maintain, upgrade, test, and perform system integration for OHTA's video teleconferencing systems (e.g. room, desktop, etc), facilities, and networks.
- Plan, submit for approval, and implement changes to OHTA's voice network architecture and infrastructure.

2.12.13 Communications and Connectivity Maintenance and Support.

Perform network communications and connectivity maintenance, including coordination with agency groups, telephone companies, internet service providers (ISP), and maintenance vendors to acquire, install, integrate, coordinate, and resolve data communication and connectivity issues and problems. The Contractor's responsibilities shall include, but are not limited to, providing the following networks support services:

- Provide engineering and technical support in the design, development, implementation, and maintenance of OHTA's data network and network services.
- Operate and administer OHTA's network infrastructure including: switches, routers, network monitoring and management systems.
- Operate and administer network components of OHTA's cyber infrastructure that may include: firewalls, intrusion detection and prevention systems, content filtering/monitoring, file integrity monitoring, centralized log store, and other network/system monitoring tools.
- Conduct special projects involving evaluation, development, and application of network and information security technology.
- Perform remedial maintenance, as required and periodic preventive maintenance on OHTA's data communications cable plant.
- Install, move, configure, maintain, monitor performance, test, diagnose, and resolve performance issues for all network hardware and software components.
- Coordinate circuit implementation and performance of communication networks with commercial vendors or other providers, resolve substandard communications performance in a timely manner, analyze hardware and software, and develop conceptual designs.
- Develop and implement network contingency and evaluation plans.
- Maintain accurate as-built drawings of the OHTA networks and cable plant.
- Provide resource utilization and capacity planning support. This should include, but not be limited to, base-lining utilization of network resources, monitoring of network resources to identify utilization/consumption trends, and projecting when resource utilization/consumption will be such that delivery of network services falls below acceptable performance levels. Provide recommendations for network component

	Document No. D11PDI8655	Document Title OHTA- IT Support Services	Page 22 of 82
--	----------------------------	---	---------------

(hardware, software, service) replacement, upgrade, and enhancement to prevent the network service performance from falling below the acceptable levels.

2.13 Information Technology Hosting/Housing Environment Support

2.13.1 The Contractor's responsibilities shall include, but are not limited to providing the following support for Information Technology Hosting/Housing Environment Support:

- a) Monitor computer facility systems to ensure maximum availability of the IT services they provide. Upon detection of problems or failures, perform remedial actions to stabilize or restore the associated IT services.
- b) Operate and administer the components of OHTA's cyber security infrastructure that may include: firewalls, intrusion detection and prevention systems, content filtering/monitoring, file integrity monitoring, centralized log store, and other network/system monitoring tools.
- c) Run and technically support production jobs in accordance with defined schedules and in compliance with current policies and procedures. This support includes, but is not limited to, hardware maintenance, software maintenance, and performing database maintenance procedures including database backups and restores. These elements and schedules shall be established to minimize negative impacts on the user community.
- d) Operate and maintain hardware and operating system software for database, file, print, application, batch and web servers, and email systems.
- e) Operate and maintain the OHTA domain controllers, including user accounts and access controls.
- f) Administration of license servers.
- g) Provide engineering and technical support in the design, development, implementation, and maintenance of OHTA's Information Technology Hosting/Housing Environment.
- h) Provide consultation for unique requirements and needs of OHTA server systems.
- i) Maintain the patches, updates and version control for OHTA servers.
- j) Perform server backups to provide for system restoration, file and database recovery, and disaster recovery. These elements and schedules shall be established to minimize negative impacts on the user community.
- k) Recover, reload, and restore files, server volumes, and databases as required to maintain maximum availability of required data, engineering design documents, and configuration data.
- l) Develop, maintain, and test each calendar year a Disaster Recovery Plan (DRP) for the OHTA computer facilities and systems. The test plan and schedule will be pre approved by the OHTA CIO. The Contractor will certify to, and receive documented approval from, the COTR that the test was satisfactorily completed.
- m) Conduct a comprehensive preventive maintenance (PM) program for OHTA hardware and software. These PM activities shall be developed and implemented in a manner consistent with industry standards and guidelines, and manufacturer-recommended maintenance schedules. These elements and schedules and the methods utilized in performing PM activities must minimize any negative effect on the user community.
- n) Provide resource utilization and capacity planning support. This should include, but not be limited to, base-lining utilization of server resources (CPU, memory, storage space, backup capacity), monitoring of the server resources to identify utilization/consumption trends, and projecting when resource utilization/consumption will be such that delivery of services by the servers falls below acceptable performance levels. The Contractor shall provide

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 23 of 82
--	----------------------------	---	---------------

recommendations for server and server component (hardware and software) replacement, upgrade, and enhancement to prevent server services from falling below acceptable levels.

2.14 System(s) Development.

Systems planning, design, development, implementation, and maintenance – software development lifecycle.

2.14.1 Requirements Analysis.

The Contractor shall analyze Government requirements to identify software and hardware specifications suitable for satisfying Government needs. They shall include, but are not limited to, discussions of applicable state-of-the-art technology and a complete analysis and reengineering of collected business process requirements for new, enhanced or expanded systems. The Contractor shall include a list of known impacts on existing systems and should note any potential problems between new or existing components, make recommendations for problem resolution to ensure compatibility. To help identify these requirements, the Contractor may use, but is not limited to, client interviews, questionnaires and site survey information. The Contractor shall consider proposed system life/cycle, opportunities for economy and efficiency, performance measurement and monitoring, expandability and upgradability, system integration/migration and cost/benefit analysis.

2.14.2 System Design.

The Contractor shall develop systems encompassing an overall system architecture including hardware, firmware, and software. The Contractor shall account for and provide services for application development and enhancements and the preparation of detailed systems designs. Systems design shall include, but not be limited to, detailed data and process models and documenting program and interface specifications, screen and report designs, prototypes, program control specifications, structure charts, module definitions, data definitions, and compilation instructions for system regeneration. The contractor shall develop a project plan with milestones, define a conceptual and detailed system design, and document system requirements.

2.14.3 Development Support.

The Contractor shall provide system development services by preparing plans, analyzing requirements, documenting specifications, designing system configurations, writing application code, conducting requirements and integration tests, writing documentation, and training personnel to provide an effective, efficient, technical solution.

2.14.4 Test and Evaluation Master Plan.

The Contractor shall write Test and Evaluation Master Plans (TEMPs) to verify design objectives and to ensure that all functional and technical requirements are satisfied. The TEMP shall include consideration of system integrity, mission criticality, acceptable performance levels and evaluation of testing resources. The Contractor shall deliver all test results to the Government for a record of the component, integration and system testing. This will also include all aspects of the design, development, documentation and testing of applications and their infrastructures.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 24 of 82
--	----------------------------	---	---------------

2.14.5 System Testing.

Develop test plans and conduct structured testing in the following areas: functional, unit, system, interface, alpha, beta, and integration tests. The contractor will prepare and submit a test analysis report and correct all discrepancies found during the testing period prior to system acceptance/accreditation or as agreed with the Technical Services Group.

2.14.6 Acceptance Testing.

The Contractor shall perform acceptance testing using both test and live data. The Government will provide the applicable standards and procedures in individual task orders. Tasks in this area include conducting the acceptance testing, making modification and corrections where appropriate and ensuring that performance standards are met in a production environment.

2.14.7 System Implementation.

Perform implementation, operations and life cycle maintenance of all aspects of the systems and technology implementations including web page development, database development, and coordination with other DOI groups, and COTS vendors.

2.14.8 Systems Specifications Documentation.

The Contractor shall document the outcome of the requirements analysis. The document shall detail the engineering, qualification requirements, and design of the system and available sources. The Contractor shall use this document as the basis for the design and formal testing of the system.

2.14.9 Development Environment.

Developers and development environment systems shall operate on segregated or isolated subnets or networks from the production environment. Due to the size of OHTA's IT operations, the production application administrators and DBAs can also be assigned as developers. Developer USERIDs shall function solely in the development environment. Developers shall have a second USERID that works in the production environment with user privileges.

2.15 Database Support

2.15.1 Database Development and Management.

The contractor shall provide the database development and maintenance support for all the software development related activities. The database development activities should include, but not limited to, database requirements collection, database requirements analysis, database design and modeling, database scripting, creating data marts and data warehouses.

2.15.2 Database Maintenance and Management.

The Contractor shall maintain the ART databases. The Contractor shall provide database tuning to optimize database performance for the ART databases. All performance tuning efforts shall be coordinated with the Government and scheduled with appropriate boards in advance of each effort. The Contractor shall manage database schema objects on the ART production databases, and also development and test databases on the development and production servers.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 25 of 82
--	----------------------------	---	---------------

2.15.3 Database Maintenance.

- a) The Contractor shall maintain all production databases by keeping them current, up and running, provide troubleshooting and resolution of database problems, and curtail potential problems. The contractor shall also maintain development and test databases servers.
- b) The Contractor shall adhere to proposed schedules and timelines for database object creations and modifications.
- c) The Contractors shall support any impacts to the ART, databases when MS SQL Server upgrades are implemented at OHTA.
- d) The Contractor shall respond to high priority database trouble calls and resolve the problems immediately.
- e) The Contractor shall manage schema objects to include creation and maintenance of tables, views, synonyms, indexes, triggers, constraints, links and any other objects required for database support.
- f) The Contractor shall create and maintain up-to-date-dictionary reports for all database schema objects.
- g) The Contractor shall manage data control to include data validation and integrity, export and import of data and other types of data loading and sweeps.
- h) The Contractor shall respond to tasking for troubleshooting of data problems. This includes research and data correction and sweeps when necessary.
- i) The Contractor shall respond to tasking for specific data report writing. This includes end of year reports and other special reports requested by the government.
- j) The Contractor shall adhere to proposed schedules and timelines for requested reports, for exports, imports and other types of data loading or migration and for data correction, modifications or sweeps.
- k) Respond to tasking for troubleshooting of DBMS problems. This includes 24x7 on-call support for ART. The contractor will be required to carry a cell phone.
- l) Upgrade newer versions of MS SQL Server and create new instances when requested by the government.
- m) Perform as database liaison with other organizations.
- n) Add user accounts to the databases after system access request forms have been filled out with appropriate Government approval.
- o) Perform imports, exports and other types of data loading and migration.

2.15.4 Database Management

2.15.4.1 Database Administration.

The Contractor shall provide database management and administration to the ART database. The Contractor shall perform system backups, database user administration, storage management, security management, table and index maintenance, and all aspects of database management and administration.

2.15.4.2 Database Population.

The Contractor shall support the Data Source Manager in data loading according to the Government furnished Data Management Plan. The Contractor shall write and maintain a

Standard Operating Procedure (SOP) for each source identified as an input to the Data Management Plan

2.15.4.3 Data Porting.

The Contractor shall write the necessary routines and support the process of moving data between the ART database and other designated databases according to the Data Management Plan. Implementation shall be based on field definition/information provided by the Government through the COTR or the CCB.

2.15.5 Database Security and Auditing

The contractor shall maintain secure databases and run audit trails. The following are specifics:

- a) Ensure that users are given accounts with the correct privileges and protected passwords.
- b) Audit database activity, as required, and archive the audit records periodically so that the SYSTEM tablespace OHTAs not fill up.
- c) Protect the databases from illegal access from remote or local users.
- d) Provide a Security, Test and Evaluation (ST&E) that conforms to security's specifications, for new databases.

2.15.6 Database Backups and Recovery

The contractor shall ensure that backups are done so that the databases can be recovered with **no** data lost. Efforts involve the following specifics:

- a) Monitor all database backups to ensure that they are running properly and can be restored if required. If the database is in archive mode, then the contractor shall monitor and switch archive logs so that they will not fill up disks. Archive logs should be copied to tape if necessary.
- b) Develop, document and implement a database backup plan for the databases that do not have backups or do not have feasible backups. This includes writing an SOP, if required, for ADP operations to assist with the backups. All backup plans shall be tested to ensure that the database can be restored.
- c) Restore databases to full operational mode when recovery is necessary.

2.16 Internet and Intranet Publishing and Management

The contractor shall provide all necessary personnel to fully support the publishing and publishing management of OHTA's Internet and Intranet. Publishing shall be in accordance with Government approved style templates. Personnel performing this task will be required to gain a working knowledge of the current Internet and Intranet sites, and our internal and external communication preferences. The Contractor's responsibilities shall include, but not be limited to, providing the following support for Internet and Intranet Publishing and Publishing Management services:

- a) Develop working relationships with the Governments Internet site managing editor, content owners and content authors to support their publishing and publishing management. The contractor shall also provide support to users by utilizing relevant enterprise tools such as a web content management system.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 27 of 82
--	----------------------------	---	---------------

- b) Perform architecture layout and design, navigational design and management, site integrity checking, HTML coding, graphic design, and digital file manipulation.
- c) Control the organization's published sites, the underlying technical infrastructure, user administration, approval, publishing, rollbacks, and site administration. The contractor shall also serve as the Intranet site managing editor, responsible for reviewing the entire intranet web site for consistency and timeliness of information.

2.17 Configuration Management.

2.17.1 Configuration Management.

The Contractor shall follow standard CM practices in updating the code, maintaining the baseline, and releasing new versions of the software. The Contractor shall participate in OHTA Configuration Control Board (CCB) and other related working group meetings. The Contractor shall support the meetings and CCB by recording the activity and the action items.

2.17.2 Configuration Management Librarian.

The Contractor shall maintain copies of baseline software and documentation and control all changes made to the baseline. This constitutes the software/documentation librarian function. Contractor is solely responsible for the timely and accurate backup of the software and documentation under its control and shall not hold the Government responsible for loss of such data. The ability to determine that the programs delivered under contract can be reproduced and that source code is not "lost" or has to be reverse engineered at a future date is critical. Program costs can easily escalate without proper CM. To ensure that CM procedures are being adhered to, the Government will institute random configuration audits.

2.17.3 Configuration Inventory Management.

The Contractor shall maintain and update configuration inventory that conforms to OHTA's standard documentation and operating procedure formats and instructions. This product shall indicate the hardware, software, and specialized products that have been installed on each of the workstations and servers. Updates shall be performed quarterly to reflect the transfer or reassignment of software or products and shall also indicate the repair status of all workstation materials. Associated license material and documentation shall also be maintained.

2.17.4 Configuration Control Board (CCB) process.

The Government will use the Configuration Control Board (CCB) process to approve the implementation of system changes.

2.17.5 Engineering Change Proposals (ECPs).

The Contractor developed ECP for that system version release shall include the description of requirements/CR in the release, cost/level of effort, and calendar time estimates for completion. It shall also include special Contractor constraints if they exist. The Contractor shall assist the Government project managers staff the ECP through the CCB process for approval.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 28 of 82
--	----------------------------	---	---------------

2.17.5.1 Approved ECPs.

Approved ECPs shall include testing, user approval, implementation, user training, and documentation. The Contractor shall complete all required security documentation for each new version release. The Contractor Team Leader shall discuss the version release status and any problems encountered with the release and the project manager at weekly meetings.

2.17.5.2 Emergency and Unscheduled CRs.

Emergency CRs, defined as those CRs that create system outages, shall be handled on a case by case basis but will require immediate attention from both the Government and Contractor with paper work to follow.

2.17.6 Contractor Proposed Enhancements.

Additionally, the Contractor shall propose enhancements to provide better and/or faster functionality in for OHTA systems. All enhancements shall be coordinated, scheduled, and approved by the Government in advance of each effort. The Government will use CRs to describe specific tasks, standards for maintenance, and specific deliverables.

2.17.7 Configuration Management Provisions for System Developers.

The Contractor shall ensure that information system developers create and implement a configuration management plan that:

- a) controls changes to the system during development,
- b) tracks security flaws,
- c) requires authorization of changes, and
- d) provides documentation of the plan and its implementation.

2.18 End-User Support and Inventory Management Support.

2.18.1 End-User Support.

The Contractor shall operate an on-site helpdesk/end-user support during standard hours of operation, with a technically knowledgeable, courteous, and responsive staff. The role of the helpdesk/end-user support will be to resolve questions concerning the application software, hardware, and network access used at OHTA; log and track requests for resolution of hardware, software, and network access problems; and handle installation, maintenance, and repair/replacement of hardware and software applicable to end users. The Contractor's responsibilities shall include, but are not limited to, providing the following support:

- a) Record, assign and track all support calls to the IT support Help Desk.
- b) Quickly respond and resolve service problems by phone to the maximum extent possible and at the client station when required. Users and OHTA CIO/COTR shall be kept informed on the progress of the action.
- c) Provide on-site repairs for desktop computers, printers, monitors, and other peripherals. Repairs will consist primarily of component replacement. Complex repairs will be accomplished off-site by a Government-designated vendor. The Contractor will track equipment repaired off-site to ensure that work is done in a timely manner.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 29 of 82
--	----------------------------	---	---------------

- d) Coordinate and support the installation, service, technical consulting, and repair of desktop computers, printers, terminals, workstations, and other computing resources.
- e) Maintain and operate a central repository for providing, maintaining, and managing a "loaner pool" of laptop computers.
- f) Develop and maintain user help guides, as required. Develop and conduct user training of supported hardware and software based on guidance from the IT Division.
- g) Notify users and key OHTA personnel of planned and unplanned outages of systems, networks, and other major components.
- h) Maintain a detailed inventory of user assigned, and issued, desktop equipment, e.g., workstations, printers, scanners, external CD-RW, external DVD, Mobile Internet Devices, cell phones, etc.
- i) Image, deploys, and maintains computers and laptops to users in a timely manner, as required.
- j) Install and maintain network and personal printers and other peripheral devices as required.

2.19 Asset Management and Inventory Support.

The Contractor shall provide asset management support services using DOI guidelines and maintain inventory for hardware and software according to OHTA property management support policy. These services shall include but not be limited to:

- a) Tagging of equipment.
- b) Coordination with administrative divisions.
- c) Procurement support.
- d) Property receipt, control and accountability.
- e) Inventory documentation.

2.20 Security

The Contractor shall follow the Department of the Interior (DOI), Information Technology Security Policy Handbook (latest version), Security Directives and the National Institute of Standards and Technology (NIST) Special Publications in their management of information security. Please refer to the current NIST Special Publications website located at:

<http://csrc.nist.gov/publications/nistpubs/>

2.20.1 Information Systems Security Manager

The Information Systems Security Manager (ISSM) responsibilities shall include, but are not limited to, providing the following support:

- a) Serve as the Point of Contact (POC) for all OHTA systems security matters;
- b) Provide subject matter guidance to OHTA personnel;
- c) Participate in the process and monitor to ensure that all OHTA systems are Certified and Accredited prior to actual operation and that they are assessed annually and reaccredited every three years or when a significant system change occurs that impacts the system's security posture;
- d) Implements departmental security policy and procedures;
- e) Participate as a permanent member of system development teams, telecommunications planning, and System Development Life Cycle (SDLC) processes;

- f) Conduct internal audits of all IT systems to ensure compliance with federal and departmental policy and procedures;
- g) Participate in general and role-based security training to enhance knowledge and skill level;
- h) Proactively coordinate the establishment of enterprise common security controls and system security controls to protect information using authentication techniques, encryption, firewalls, access controls, and comprehensive departmental Incident Response Procedures with all System Administrators (SA) and business process owners in alignment with DOI enterprise architecture, NIST SP-800-30 Risk Management Guide for Information Technology Systems and using controls identified in NIST 800-53 Rev. 1 Recommended Security Controls for Federal Information Systems, NIST 800-35 Guide to Information Technology Security Services and NIST 800-27 Engineering Principles for Information Technology Security (A Baseline for Achieving Security), Revision A;
- i) Coordinate with business process owners to categorize information systems and determine sensitivity levels and document in SSP leveraging DOI enterprise architecture to identify impacts to business processes, NIST FIPS-199 Standards for Security Categorization of Federal Information and Information Systems and SP-800-30 Risk Management Guide for Information Technology Systems;
- j) Collaborate with system owners to ensure that contingency plans for all OHTA IT systems are established, tested and aligned with Site, OHTA, and DOI strategies and NIST 800-34 Contingency Planning Guide for Information Technology (IT) Systems;
- k) Ensure compliance with backup, storage and media sanitization and disposition policies and guidance using NIST 800-88 Guidelines for Media Sanitization and FIPS 200, (Minimum Security Requirements for Federal Information and Information Systems) and DOI Media handling policy;
- l) Monitor physical spaces to ensure that the security requirements of IT Restricted Space are followed in maintaining, updating or planning new space, and advise the CIO if space does not meet security requirements;
- m) Ensure that all personnel are appropriately trained in the security Rules of Behavior (ROB) prior to being granted access to systems;
- n) Participate in the development of a security architecture for IT systems;
- o) Monitor and coordinate patch management and scanning techniques for all systems;
- p) Participate in identification and mitigation of all system vulnerabilities,
- q) Coordinate the provisioning of security controls for PEDS and other wireless technology;
- r) Participate in the overall OHTA Security Plan for the program and coordinate with ISSO to ensure that current system specific plans are in place for all IT systems;
- s) Coordinate or participate in risk assessments of systems and mitigate vulnerabilities;
- t) Monitor CM practices to ensure that security controls are maintained over the life of the IT systems, and formulate and prepare an electronic inventory for OHTA computing devices;
- u) Monitor and participate in assessments to ensure that privacy requirements are met;
- v) Plan and document security costs for IT investments and systems;
- w) Prepare and update reports to ensure that the OHTA complies with mandated internal and external security reporting requirements, including FISMA and CPIC;
- x) Proactively participate in new Cyber Security initiatives including, but not limited to, computer investigations and forensics;
- y) Prepare and coordinate Incident Responses with the Chief Information Security Officer (BCISO) to include all associated actions necessary to mitigate the risk to OHTA systems.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 31 of 82
--	----------------------------	---	---------------

- z) Ensure annual Contingency Plan (CP) and Security Control Testing for each system.
- aa) Serve as a POC for system users with security issues;
- bb) Coordinate security program and system elements with the OHTA IT Program Managers by evaluating system environments for security requirements and controls including: IT Security Architecture, hardware, software, telecommunications, security trends, and associated threats and vulnerabilities;
- cc) Manage security controls to ensure confidentiality, integrity and availability of information;
- dd) Build security into the system development process and define security specifications to support the acquisition of new systems;
- ee) Review and sign off on system procurement requests to ensure that security has been considered and included;
- ff) Serve as a key advisor in risk assessments of their assigned systems and mitigate vulnerabilities for these respective systems;
- gg) Adhere to CM practices to ensure that security controls are maintained over the life of IT systems;
- hh) Update the IT asset inventory for all computing devices;
- ii) Adhere to and implement system security controls that ensure the protection of SBU information using authentication techniques, encryption, firewalls, and access controls;
- jj) Assist the BCISO in following departmental Incident Response procedures;
- kk) Document all procedures according to departmental and OHTA standards;
- ll) Routinely monitor and examine application, system and security logs for security threats, vulnerabilities and suspicious activities;
- lll) Report suspicious activities to the BCISO, and OHTA CIRT/CIRC.

2.20.2 The Contractor Information Resources Management (IRM), Systems Operations & Maintenance Staff, and Programming Staff shall:

- a) Be knowledgeable of federal and OHTA security regulations when developing functional and technical requirements;
- b) Coordinate security program and system elements with the OHTA IT program managers and BCISO by evaluating system environments for security requirements and controls including: IT security architecture, hardware, software, telecommunications, security trends, and associated threats and vulnerabilities;
- c) Manage security controls to ensure confidentiality, integrity and availability of information;
- d) Build security into the system development process and define security specifications to support the acquisition of new systems;
- e) Assist with defining security controls and associated costs in the CPIC process;
- f) Assist the system owner and BCISO in the C&A process, including updates to the overall OHTA SSP;
- g) Participate in risk assessments of all systems and mitigate vulnerabilities;
- h) Adhere to CM practices to ensure that security controls are maintained over the life of IT systems;
- i) Update the IT asset inventory for all bureau computing devices;
- j) Adhere to and implement system security controls at the appropriate Common Criteria EAL for the level of sensitivity of the information housed on the system and ensure the protection

	Document No. DI1PD18655	Document Title OHTA- IT Support Services	Page 32 of 82
--	-----------------------------------	--	---------------

of SBU information using authentication techniques, encryption, firewalls, and access controls;

- k) Assist the BCISO in following department Incident Response procedures;
- l) Assist the system owner and BCISO in the development, testing and maintenance of OHTA and system Contingency Plans, backup and storage procedures;
- m) Document all procedures related to operational roles and responsibilities according to departmental and bureau standards;
- n) Routinely monitor and examine application, system and security logs for security threats, vulnerabilities and suspicious activities;
- o) Report suspicious activities to the bureau ITSP office; and assist the BCISO in any other security related duties, as required.

2.20.3 Account Management

The Contractor shall manage all information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The Contractor (ISSM) shall review at least every 3 months information system accounts.

2.20.4 Separation of Duties

The Contractor shall ensure that information systems enforce separation of duties through assigned access authorizations. The Contractor shall ensure that assignment of security responsibilities must follow the principle of “separation of duties”. The following three categories of “duty” must be kept separate or compensating controls in place to monitor activity closely.

- IT administration or operation (assuring systems function, to serve the system users);
- IT security (assuring adequacy of system controls for availability, integrity, and confidentiality); and
- IT management (allocating adequate resources for implementation of effective IT security programs and system controls).

2.20.5 System Audit Records.

The Contractor shall ensure that at a minimum, all information systems generate audit records for the following events:

2.20.5.1 System-Level Audit Events.

If a system-level audit capability exists, the audit trail should capture, at a minimum, any attempt to log on (successful or unsuccessful), the log-on ID, date and time of each log-on attempt, date and time of each log-off, the devices used, and the function(s) performed once logged on (e.g., the applications that the user tried, successfully or unsuccessfully, to invoke). System-level logging also typically includes information that is not specifically security-related, such as system operations, cost-accounting charges, and network performance.

2.20.5.2 Application-Level Audit Events.

System-level audit trails may not be able to track and log events within applications, or may not be able to provide the level of detail needed by application or data owners, the system administrator, or the computer security manager. In general, application-level audit trails monitor

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 33 of 82
--	----------------------------	---	---------------

and log user activities, including data files opened and closed, specific actions, such as reading, editing, and deleting records or fields, and printing reports. Some applications may be sensitive enough from data availability, confidentiality, and/or integrity perspective that a "before" and "after" picture of each modified record (or the data element(s) changed within a record) should be captured by the audit trail.

2.20.5.3 User Audit Events.

User audit trails can usually log:

- a) all commands directly initiated by the user;
- b) all identification and authentication attempts; and files and resources accessed.
- c) It is most useful if options and parameters are also recorded from commands. It is much more useful to know that a user tried to delete a log file (e.g., to hide unauthorized actions) than to know the user merely issued the delete command, possibly for a personal data file.

2.20.5.4 Response to Audit Processing Failures.

The Contractor shall ensure that information systems are configured to alert appropriate personnel in the event of an audit processing failure (e.g., software/hardware error, failure in the audit capturing mechanism, or audit storage capacity being reached or exceeded), and shuts down the information system or overwrites the oldest audit records.

2.20.6 Baseline Configuration

The Contractor shall:

- a) Document and maintain a current baseline configuration of all information systems, an inventory of all system's constituent components, and relevant ownership information; and
- b) Comply with the requirements specified under CA-1, *C&A Implementation Methodology*, regarding implementation of baseline security configurations based on the NIST SP 800-53 controls, applicable Security Technical Implementation Guides (STIGs), and associated requirements specified within this policy handbook for all major operating systems, database systems, web-based systems, applications, and other types of configurable network devices and IT resources.

2.20.7 Incident Response Training

The Contractor personnel shall be trained in their incident response roles and responsibilities with respect to all information systems and provide refresher training, at least annually.

2.20.8 Incident Response Testing and Exercises

The Contractor shall test (live exercise) the incident response capability for all information systems at least annually using tests/exercises defined in the OHTA procedures to determine the incident response effectiveness and document the results.

2.20.9 Physical Access Control.

The Contractor shall ensure for server rooms, communications centers or any other areas within a facility containing large concentrations of information system components that controls for the physical access to the information system are independent of the physical access controls for the facility.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 34 of 82
--	----------------------------	---	---------------

2.20.10 Applicable Standards.

Contractors must follow the DOI System Development Life Cycle (SDLC), NIST SP 800-64 and the DOI SDLC Security Integration Guide.

2.20.11 Security Categorization.

The Contractor must use the FIPS 199 and the NIST SP 800-60 for all systems to determine information types and security categorization based on mission impact, data sensitivity, risk level, and office/departmental/ national criticality.

2.20.12 System Security Plan (SSP).

The Contractor shall develop, maintain, and implement a security plan for all information systems that provides an overview of the security requirements for the system and a description of the security controls in place or planned for meeting those requirements. Contractors shall ensure that the security control requirements in the SSP are in compliance the current version of NIST SP 800-53. The OHTA CIO will review and approve the plan.

2.20.13 Security Control Compliance.

Contractors shall ensure continuous compliance with the security control requirements documented in the System Security Plans (SSP).

2.20.14 Certification and Accreditation Support.

All of OHTAs Major Applications and General Support Systems must be certified and accredited (C&A) prior to going into production and reaccredited every three years or whenever there is a major change that affects security.

2.20.14.1 The Contractor shall produce C&A supporting documentation in accordance with NIST SP 800-37, 800-18, Rev.1, 800-30, 800-60 vol. 1 and vol. 2, 800-53, Rev.1 - Annex 1, Annex 2 and Annex 3, FIPS 199 and FIPS 200, the associated DOI guides/templates, the DOI Security Test & Evaluation (ST&E) Guide, and the DOI Privacy Impact Assessment.

2.20.14.2 The Contractor shall provide assistance to the government personnel or an independent contractor who will conduct the Certification and Accreditation, Security Test & Evaluation (ST&E). The contractor will take appropriate and timely action to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

2.20.15 Annual Security Control Assessment

2.20.15.1 The contractor must conduct an annual security assessment in accordance with annual DOI guidance on all information systems in production.

2.20.15.2 Both hard copy and electronic copies of the assessment will be provided to the COTR.

2.20.15.3 The Contractor shall provide assistance to the government personnel or an independent contractor who may also conduct an independent annual security control assessment.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 35 of 82
--	----------------------------	---	---------------

2.20.15.4 The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

2.20.16 Internet Logon Banner.

The Contractor shall ensure that the DOI-approved internet logon banner is displayed on the first page of any publicly accessible web pages owned by DOI/OHTA. The information contained in the banner is standard and must be approved by DOI legal staff.

2.20.17 Incident Reporting.

The contractor must report computer security incidents affecting DOI data or systems in accordance with the DOI Computer Incident Response Guide.

2.20.18 Quality Control.

All software or hardware purchased must be free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc. The Contractor shall provide written certification upon delivery that the software and/or hardware free of malicious code such as viruses, Trojan horse programs, worms, spyware, etc. Malicious code or malware is defined as software (or firmware) designed to damage or do other unwanted actions on a computer system. Examples of malware include viruses, worms, Trojan horses and spyware. Viruses, for example, can cause havoc on a computer's hard drive by deleting files or directory information. Spyware can gather data from a user's system without the user knowing it.

2.20.19 Logon Banner.

Contractor employees who access DOI information systems must acknowledge a government-approved legal warning banner prior to logging on to the system. This includes contractor owned information systems hosting DOI data. The network warning banner communicates that there is no expectation of privacy in the authorized or unauthorized use of DOI information systems. The use of warning banners on DOI computers and networks provides legal notice to anyone accessing them that they are using a U.S. Government system that is subject to monitoring. Users should also be notified of the possible sanctions, such as loss of privileges or prosecution, if they misuse or access the network without authorization. All DOI systems must display warning banners upon connection to such system. These banners will display a warning that states the system is for legitimate use only, is subject to monitoring, and carries no expectation of privacy. DOI networks and information systems do not inherently provide users a right of privacy. As such, the DOI reserves the right to monitor use in accordance with Information Security Program policies. System Owners must notify users of monitoring prior to system access to avoid any question about an implied right to privacy on the system. The information contained in the banners is standard and must be approved by DOI's legal staff. All DOI computers, workstations, laptops and other information resources will display a standard, DOI approved legal banner.

2.20.20 Annual Systems Risk Assessment.

The Contractor shall participate in the annual risk assessment for all OHTA information systems.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 36 of 82
--	----------------------------	---	---------------

2.20.21 Developer Security Testing-The Contractor shall ensure that information system developers create a security test and evaluation plan, implement the plan, and document the results. The Contractor shall utilize developmental security test results to the greatest extent feasible after verification of the results, recognizing that these results are impacted whenever there have been security relevant modifications to the information system subsequent to developer testing. Developmental security test results may be used in support of the security certification and accreditation process for the delivered information system.

2.21 Vulnerability and Patch Management

2.21.1 Vulnerability Management

2.21.1.1 Vulnerability Scanning.

All systems must be scanned monthly using the Government provided vulnerability analysis tool and in accordance with the OHTA vulnerability and patch management plan. All “safe” or “non-destructive” checks must be turned on. An electronic copy of each report and session data will be provided to the COTR.

2.21.1.2 Independent Vulnerability Scans.

The government will reserve the right to conduct unannounced and prearranged independent vulnerability scans using government personnel or another contractor.

2.21.2 Security Patch Management Program.

The Contractor shall implement a uniform system of patch management for all IT systems, devices and appliances, regardless of operating system or platform for OHTA IT environment in accordance with Department of Interior patch management requirements and the OHTA Security Procedures.

The Contractor shall use the installed enterprise vulnerability scanning solution. The Contractor will designate someone on the O&M Staff as the Patch Management Officer.

2.21.3 Corrective Actions.

The contractor will take appropriate and timely action (this can be specified in the contract) to correct or mitigate any weaknesses discovered during such testing, generally at no additional cost.

2.22 Contingency Planning and Management.

2.22.1 Contingency Plan.

The Contractor shall develop and implement contingency plans (in accordance with NIST SP 800-34 and the DOI Contingency Plan Guide) for all information systems that address contingency roles, responsibilities, assigned individuals with contact information, and activities associated with restoring the system after a disruption or failure. The Contractor will submit the Plan in accordance with section 17 of the SOW. the OHTA CIO will review and approve contingency plans and distribute copies of the plan to key contingency personnel.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 37 of 82
--	----------------------------	---	---------------

2.22.2 Contingency Plan Testing and Exercises.

The Contractor shall:

- a) Conduct an exercise testing the contingency plan for information systems annually, using OHTA developed tests and exercises to determine the plan's effectiveness and the organization's readiness to execute the plan;
- b) The exercise must be conducted during the May/June time frame and
- c) Review the contingency plan test/exercise results and initiate corrective actions.

2.23 Recommend Emerging Technologies.

As directed, evaluate hardware, firmware, peripherals, software packages for potential use by OHTA, and provide recommendations for their integration into the environment.

2.24 Reporting Requirement/Delivery Schedule

2.24.1 Plans

The Contractor, by preparing plans, designing system configurations and training personnel shall provide an effective, efficient technical solution which meets the IT needs of the Government. Documents will be provided to the Government upon request for review, update and incorporation into existing plans. The Contractor may be required to provide the following plans:

- a) **Project Management Plan.** The contractor shall prepare a Project Management Plan describing the technical approach, organizational resources, and management controls to be employed to meet the cost, performance and schedule requirements for this effort. The Project Management Plan shall detail the products, methods for developing the products, allocation of staff and other resources necessary to produce the products, and a revised timeline for producing the products, if necessary. The Contracting Officer's Representative (COTR) shall receive the revised Project Management Plan in both hard copy and electronic form (Microsoft Word). Based on the Project Management Plan, the COTR will provide approval to move forward on planned activities. The contractor shall request prior approval on all activities not included in the plan or any modifications to the plan after approval has been given.
- b) **Work Plan.** The contractor shall produce a work plan for each major initiative being supported. The plan will include a project management sheet identifying related tasks, critical path and proposed start and completion timeframes. The contractor shall get the approval from COTR before starting the work on the work plan. The work plan should also include an estimated cost of the project.
- c) **Implementation Plan.** The Contractor shall develop an implementation plan based on the system design to ensure that all implementation activities are completed in a timely and accurate manner. The issues and approaches considered shall encompass a variety of sources such as external audits, technical reports, Federal standards, technical guidelines, operational policies and doctrines.
- d) **Maintenance Plan.** The Contractor shall develop a maintenance plan based on the system design. The plan shall include project completion support procedures, and policies and guidelines for maintaining the system and individual software and hardware components. The plan shall include, but not be limited to, procedures for parts repair and replacement, preventative maintenance, end user support, and problem resolution.
- e) **Configuration Management Plan.** The Contractor shall provide a Configuration Management (CM) plan that describes the implementation of configuration management activities, procedures

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 38 of 82
--	----------------------------	---	---------------

and IT standards. The CM plan should address, but is not limited to, configuration controls, review procedures, item identification, audits, baseline management and status accounting record keeping.

f) Quality Assurance Plan. The Contractor shall provide a Quality Assurance (QA) Plan that describes the quality assurance activities, procedures and standards to assure the quality of each deliverable item. The Quality Assurance Plan may address, but is not limited to, the following: quality assurance evaluations, development processes, system components, documentation, acceptance inspections, reviews and audits.

g) Account Management Plan and Procedures

The contractor shall develop and maintain Account Management Procedures that includes:

- 1) Identification of account types (i.e., individual, group, and system) and establishment of conditions for group membership, and assignment of associated authorizations.
- 2) Identification of authorized users of the information system and specified access rights/privileges.
- 3) Identify access granted to the user based on:
- 4) a valid need-to-know that is determined by assigned official duties and satisfying all personnel security criteria; and
- 5) intended system usage.
- 6) Account creation procedures, including procedures for supervisor account request and approval;
- 7) Procedures and timeframes to notify account managers when information system users are terminated or transferred. Account managers should also be notified when users' information system usage or need-to-know changes.
- 8) Procedures to remove, disable, or otherwise secured accounts to occur within 24 hours of notification of a change in user status such as:
- 9) Departs the agency voluntarily or involuntarily;
- 10) Transfers to another bureau or office within the agency;
- 11) Is suspended;
- 12) Goes on long term detail; or
- 13) Information system usage or need-to-know changes.
- 14) Procedures for the review and auditing of accounts (federal employee, contractor, and "guest" accounts) to determine validity at least every 3 months or more frequently based on system categorization.
- 15) Procedures to remove, disable, or otherwise secure unnecessary accounts.

h) Security Test and Evaluation (ST&E) Plan

The ISSO shall develop and maintain a Security Test and Evaluation (ST&E) for each information system that identifies the information system and related devices included in the accreditation boundary to be tested and relevant test cases for each.

i) System Security Plan (SSP)

The ISSO shall develop and maintain a System Security Plan (SSP) for each information system, which shall be approved by the Government System Owner.

j) IT Disaster Recovery Plan

The contractor shall develop, document, and maintain an IT Disaster Recovery Plan

k) Incident Response Plan

The contractor shall develop, document, and maintain an Incident Response Plan

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 39 of 82
--	----------------------------	---	---------------

l) System Maintenance Plan and Procedures

The contractor shall develop, document, and maintain a System Maintenance Procedure document.

m) Developer Security Testing Plan

The Contractors system developers shall create a security test and evaluation plan, implement the plan, and document the results.

n) IT Contingency and Disaster Recovery Plans

The contractor shall develop, document, and maintain an IT Contingency and Disaster Recovery Plan.

o) Encryption Plan

The Contractors system developers shall create and maintain an encryption plan that includes:

- A configuration layout showing complete end-to-end details of the telecommunication or computer systems encryption points.
- The type of encryption to be used.
- The source of key generation and insertion for symmetrical encryption methods.
- The cryptographic period required, that is, the amount of time before a session key should be updated.
- The system procedures for key loading, key generation, key protection and distribution, key recovery, and key destruction.
- Key recovery procedures to recover encrypted sensitive information when the data is stored electronically.

2.24.2 Reporting Requirements

- a) **Weekly Status Reports.** The contractor shall submit weekly progress/status reports. The status report will be submitted (via email) to the COTR or the appointed OHTA Project Manager no later than close of business each Friday. The reports highlight the work performance and related activities accomplished during the week and the planned/expected activities for the following week. The report should also include any exceptions or deviations from the planned activities.
- b) **Monthly Project & Financial Status Report:** A monthly Project & Financial Status Report will be submitted no later than the 10th of each month. The reporting requirements will be described during the initial kick-off meeting. It is expected that these requirements will include, but are not confined or constrained to:
- 1) Hours expended during the reporting period by individual task
 - 2) Cumulative hours expended throughout the reporting period by job category
 - 3) Contract funds expended during the reporting period
 - 4) Summary of work accomplished during the reporting period, percent of total work complete, and achievement of any major milestones or submission of deliverables
 - 5) Any issues or problems impacting project progress and steps taken toward along with their resolution
 - 6) Schedule of activities planned, estimated hours for the next reporting period, and the estimated number of remaining hours to complete activities
 - 7) Future monthly financial projection
- c) **Earn Value Management (EVM) Report.** A monthly Earn Value Management (EVM) Report will be submitted no later than the 10th of each month. The Government will provide

the Contractor with the starting format for the EVM report. The Contractor can with the agreement of the Government make changes to the EVM Report format and content.

- d) **Oral Reports.** The contractor shall deliver oral progress reports as requested by the COTR or the assigned OHTA project managers. These reports shall include, but not limited to, all of the elements listed under the weekly status report.
- e) **Automated Reports.** The contractor shall provide, as and when requested, a series of automated reports that have been generated via the tracking systems. These reports include help desk reports, defect reports, and other project reports which can be extracted from the implemented tracking systems.
- f) **Program Reviews.** The contractor will conduct program reviews on a quarterly basis.
- g) **Final Report(s).** The contractor shall provide a final report to the COTR at the conclusion of each task. The report will summarize objectives achieved, significant issues, problems, and recommendations to improve the process in the future.

2.25 Deliverables/Delivery Schedule

Unless otherwise specified, the OHTA will have a maximum of ten (10) working days from the day the draft deliverable is received to review the document, provide comments back to the contractor, and approve or disapprove the deliverable(s). The contractor will also have a maximum of ten (10) working days from the day comments are received to incorporate all changes and submit the final deliverable to the Government. The contractor may assume a deliverable is acceptable if it receives no feedback within this time. All days identified above are intended to be work days unless otherwise specified.

2.25.1 Summary of Above Deliverables – Timelines

2.11.1	Risk Management Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.11.3	Quality Control Plan (QCP)/Quality Assurance Plan.	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.11.4	Technical Review Meetings System Requirements Review (SRR) System Design/Definition/Functional Review (SDR/SFR) Software Specification Review (SSR) Preliminary Design Review (PDR) Critical Design Review (CDR) Test Readiness Review (TRR) Production Readiness Review (PRR)	As directed by Project Officer.
2.11.4	Technical Review Meeting Agenda	3 days prior to meeting.
2.11.4	Technical Review Meeting Minutes	28 days following meeting
2.15.4.1	System Backups	
2.12.5.2	System Backup Test	Annual, by 1 st of June.
2.12.7.1	Maintenance Record	Recorded as Maintenance

		Occurs
2.24.1 d)	Maintenance Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.12.8	Account Management Report	Quarterly
2.24.1 g)	Account Management Plan and Procedures	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.12.11	Trusted Facility Manual (TFM)	Annually in June as plan is due.
2.12.13	Network Configuration Diagrams	Within 60 days of contract award. Updated as changes occur.
2.24.1 j)	IT Disaster Recovery Plan (DRP)	Annually in April as plan is due.
2.12.13	Requirements Documentation	As directed by Project Officer.
2.12.13	System Design Documentation	As directed by Project Officer.
2.20.14.2	Test & Evaluation Master Plan	As directed by Project Officer.
2.14.5	Test Analysis Report	As directed by Project Officer.
2.14.6	Acceptance test Report	As directed by Project Officer.
2.14.8	System Specification Documentation	As directed by Project Officer.
2.15.3	Data Dictionary	Within 90 days of contract award. Annually reviewed and updated due by 1 st of June.
2.15.4.2	Data Management Plan	As directed by Project Officer.
2.24.1 h)	DB Security, Test and Evaluation (ST&E) Plan and Report	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.15.6 b)	DB Backup Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.17.2	Configuration Management Library	Within 60 days of contract award. Updated as changes occur.
2.17.3	Configuration Inventory	Within 60 days of contract award. Updated as changes occur.
2.17.5	Engineering Change Proposals (ECPs)	As required
2.17.7	Software Developer CM Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.19	Asset Inventory	Within 60 days of contract award. Updated as changes occur.
2.15.5	Security, Test and Evaluation (ST&E)	Annually reviewed and updated by 1 st of June.

2.12.8	System Account Review Report	Quarterly
2.20.6	Baseline Configuration	Within 60 days of contract award. Updated as changes occur.
2.20.8	Incident Response test/exercise Report	Annual, by 1 st of June.
2.20.14.1	C&A Supporting Documentation	Annually reviewed and updated by 1 st of June.
2.20.15	Security Control Assessment Report	Within 15 days after the Test.
2.20.18	Quality Control Certification(s)	When required
2.20.20	Risk Assessments	Annual, by 1 st of June.
2.20.21	Developers Security Testing Report	Within 15 days after the Test.
3.1.4	Confidentiality/Non-Disclosure Agreement	Prior to the employee starting work.
2.21	Vulnerability Scanning	Monthly
2.21	Patch Management Report	Monthly
2.22	IT Contingency Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.22	IT Contingency Plan Test & Exercise Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.22	IT Contingency Plan Test & Exercise Report	Within 15 days after the Test.
2.24.1 k)	Incident Response Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.24.1 L)	System Maintenance Plan and Procedures	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.24.1 O)	Encryption Plan	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.24.1 G)	Account Management Plan and Procedures	Within 60 days of contract award. Annually reviewed and updated due by 1 st of June.
2.24.2 a)	Weekly Status Reports.	No later than close of business each Friday.
2.24.2 b)	Project & Financial Status Report	Monthly, 10 th day of following month.
2.24.2 f)	Program Review	Quarterly
2.24.2 c)	Earn Value Management (EVM) Report	2nd business day of the month. This shall run one month behind.

SECTION 2 – Statement of Work - Attachment (1) Servers List

- 8 Dell Poweredge 2650, 1Gb – 3Gb ram, 150GB – 500GB storage, Windows Server 2003 Enterprise
- 4 Dell Poweredge 1650, 1Gb ram, 80GB - 500GB storage, Windows Server 2003 Enterprise
- 3 Dell Poweredge 6650, 3Gb – 4Gb ram, 1TB – 2TB storage, Windows Server 2003 Enterprise
- 1 Dell Poweredge 6850, 28Gb ram, 2TB storage, Windows Server 2003 Enterprise
- 1 Powervault 775N, 3Gb ram, 4TB storage, Windows Server 2003 Enterprise

- 5 IBM x3250, 3Gb – 4Gb ram, 500GB – 1TB storage, Windows Server 2003 Enterprise & Windows Server 2008 Enterprise
- 5 IBM x3650, 8Gb – 16Gb ram, 500GB – 8TB storage, Windows Server 2003 Enterprise
- 3 IBM x366, 3Gb ram, 200GB – 3TB storage, Windows Server 2003 Enterprise
- 1 IBM x346, 2Gb ram, 600GB storage, Windows Server 2003 Enterprise
- 5 IBM x3650 M2, 2Gb – 12Gb ram, 300GB – 2.5TB storage, Windows Server 2003 Enterprise

SECTION 2 – Statement of Work - Attachment (2) Workstation List

- | | | | |
|----|-------------------|----------|----------------|
| 14 | Dell E6400 Laptop | 75GB HD | 3GB RAM - XP |
| 5 | Dell D630 Laptop | 115GB HD | 2GB RAM - XP |
| 29 | Dell 760 | 75GB HD | 3GB RAM - XP |
| 15 | Dell 755 | 150GB HD | 2GB RAM - XP |
| 44 | Dell 620 | 80GB HD | 1GB RAM - XP |
| 22 | Dell 280 | 75GB HD | 512MB RAM - XP |
| 6 | Dell 270 | 75GB HD | 1GB RAM - XP |
| 23 | Dell 260 | 75GB HD | 1GB RAM - XP |
| 12 | ADS | 80GB | 1GB RAM -XP |

Section 3 – Task Order Special Provisions/ Additional Order Terms and Conditions

3.0 Personnel Oversight

Contractor Personnel

The Contractor shall be responsible for managing and overseeing the activities of all Contractor personnel, as well as subcontractor efforts used in performance of this effort. The contractor shall provide necessary and sufficient personnel to accomplish all the services within the time frames specified in this contract. Contractor personnel shall be trained, qualified, and certified under the requirements specified in this contract, and be given full knowledge of the requirements of this contract before starting work. The contractor shall assure adequate office coverage, excluding Government holidays. The contractor will provide staff for emergency support whenever deemed necessary by the COTR. The Contractor's management responsibilities shall include all activities necessary to ensure the accomplishment of timely and effective support, performed in accordance with the requirements contained in the statement of work. Resumes submitted for employees assigned to perform under this statement of work shall contain documented experience directly applicable to the functions to be performed. Further, these prior work experiences shall be specific and of sufficient variety and duration that the employee is able to effectively and

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 44 of 82
--	----------------------------	---	---------------

efficiently perform the functions assigned.

The Program Manager shall be responsible for the overall administration of the contract. The Program Manager shall plan and manage the development of multi-user systems using advanced systems engineering and state-of-the-art management methodologies, and serve as the COTR's primary point of contact with the contractor's corporate management. The Program Manager will meet periodically with the COTR and the on-site Project Manager to assure that Government needs are met according to best industry practices and standards, and that the proper resources are provided to ensure that only high quality products are delivered to the Government.

The Project Manger will attend weekly meetings, at a minimum, with the COTR to review contractor performance. These meetings may vary in frequency at the discretion of the COTR. Also, the COTR may convene meetings at any time to review the status of specific work assignments or to resolve issues raised by the Government or contractor. A mutual effort will be made to resolve all problems identified. These meetings are primarily to review anticipated deliverables and milestones that the contractor is expected to meet and to assess the timeliness and quality of the expected deliverables.

3.1 Contractor Staff

- a. The contractor is responsible for providing qualified personnel with the management, technical and subject matter expertise required to accomplish the activities and prepare the deliverables identified in this Statement of Work. The Contractor shall perform a resume review with the COTR or Government designee and may hold interviews in which the COTR or Government designee participates.
- b. The contractor shall submit in writing to the OHTA COTR, the names, resumes, clearance status, etc., of all candidates the contractor proposes to engage in work under the contract along with the labor category and hourly rate that would apply.
- c. The Government reserves the right to require (with written notification) the contractor to replace an individual whose technical skills and suitability are judged deficient.
- d. Contractor personnel shall present a neat appearance and be easily recognized as contractor employees by wearing a Security Identification Badges at all times while on Government premises. When Contractor personnel attend meetings, answer phones, and work in other situation where their status in not obvious to third parties they must identify themselves as such to avoid creating the impression that they are government employees.

3.1.1 Training

The contractor shall provide personnel/staff that is adequately trained and who have attained knowledge necessary for the performance of the client requirements. It is anticipated that contractor employees will be required by the government to attend conferences and symposiums to provide interface and attain knowledge necessary for the performance of client requirements. The attendance of training, conferences, and symposiums directed by the Government, shall be funded/billable to the Government. Training, conferences, and symposiums required keeping contractor personnel competitive; maintaining staff licenses and qualifications is the funding responsibility, the contractor.

Contractor employees must successfully complete DOI's end-user computer security awareness training prior to being granted access to Government data or being issued a user account. Periodically (usually annually or biannually), the Government may request Contractor employees completed various IT and security related awareness training that are mandatory for government employees in similar areas of employment. The Contractor shall ensure that its employees, when requested by DOI, complete the following:

- IT Security Awareness
- Privacy Act
- Records Management
- Role-Based Security Training

And others that may be mandated throughout the period of performance and any extended periods. The Contractor shall ensure that new employees complete the annual Government provided IT Security Awareness training within 10 business days after commencing work on this contract.

Additionally, the contract employees must sign a Rules of Behavior (RoB) that states they have read the appropriate Rules of Behavior and other applicable Information security policies

3.1.2 Personnel Changes.

The contractor must notify the COTR immediately when an employee working on a DOI system is reassigned or leaves the contractor's employ. For unfriendly terminations, the COTR, OHTA Personnel Security Officer, and OHTA Information Security Officer must be contacted PRIOR to the termination.

3.1.3 Background Investigations.

Contractor employees who will have access to DOI information or will develop custom applications are subject to background investigations. The level/complexity of background investigations must be the same as for a federal employee holding a similar position; DM441, Chapter 3, (http://elips.doi.gov/app_dm/index.cfm?fuseaction=tableofcontent) provides guidance for the appropriate background investigations based on types of access.

The Contractor is responsible for paying the cost the background investigations. Existing clearances at the same or higher levels may be accepted. The request forms should be included in the solicitation if possible. Work cannot begin on Government systems/information until the background investigation has at least been initiated and the National Agency Check (NAC) is completed.

3.1.4 Non-disclosure Agreement.

Contractor employees must sign a non-disclosure agreement prior to gaining access to DOI or Service information or that develops applications. Copy of agreement is attached. (Attachment 2)

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 46 of 82
--	----------------------------	---	---------------

3.1.5 Standards of Conduct / Disciplinary Actions

Each employee or supervisor of the Contractor is expected to adhere to standards of behavior, appearance, and integrity that reflect credit on themselves, their employer, and the Federal Government.

- a) The Contractor is responsible for ensuring that its employees and those of its subcontractor(s) do not disturb papers on desks of others open desk drawers of others or cabinets, use Government telephones, except as authorized, or otherwise jeopardize the security and the privacy of Government employees, its clientele, and the contents and property of the federal building(s) in which the task order work is performed.
- b) The Contractor will be responsible for taking such disciplinary action, including suspension without pay or removal from the worksite, with respect to its employees, as may be necessary to enforce those standards.
- c) The requirements of this clause must be expressly incorporated into subcontract(s) and must be applicable to all subcontractor employees who may perform recurring services or work at the federal building and grounds of this task order.
- d) The Government retains the right to permanently remove any employee of the Contractor from performing duties assigned under this task order at the federal building should the employee's performance so warrant. The Government may request the Contractor to immediately remove any employee of the Contractor from the federal building/work-site should it be determined by the Security Officer that the individual employee of the Contractor is "unsuitable" for security reasons or for otherwise being found to be unfit for performing his assigned duty at a federal building. The following areas (not all-inclusive) are considered justification for requesting the Contractor to immediately remove an employee from a federal building/work site:
 - e) Neglect of assigned duty and refusing to render assistance or cooperate in upholding the integrity of the security programs at the worksite;
 - f) Falsification or unlawful concealment, removal, mutilation, or destruction of any official documents or records, or concealment of material facts by willful omissions from official documents or records;
 - g) Disorderly conduct, use of abusive or offensive language, quarreling, intimidation by words or actions, or fighting; participation in disruptive activities which interfere with the normal and efficient operations of the Government;
 - h) Theft, vandalism, immoral conduct, or any other criminal actions;
 - i) Selling, consuming, or being under the influence of intoxicants, drugs, or controlled substances which produce similar effects;
 - j) Improper use of official authority or credentials, as a supervisor or employee of the Contractor;
 - k) Violation of agency and Contractor security procedures and regulations; and
 - l) Violation of the rules and regulations governing federal public buildings and grounds, set forth in 41 CFR Subpart 101-20.3 *Conduct on Federal Property*.
- m) Following a recommendation from an agency program official or security officer, the CO will make all determinations regarding the removal of any employee of the Contractor from and denial/termination of clearance and access to the federal building worksite for non-performance, misconduct, or failure to abide by all laws and regulations. The CO will verbally inform the Contractor about the employee, followed by a written confirmation or determination. Specific reasons for the removal of an employee will be provided to the

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 47 of 82
--	----------------------------	---	---------------

Contractor in writing. In the event of a dispute, the Contracting Officer will make a final determination.

- n) Upon a determination of the Government that an employee of the Contractor be removed from or denied access to a federal building worksite, the employee's clearance and access to the federal building must be immediately revoked or otherwise terminated. Furthermore, if applicable, the building pass and/or other access device(s) previously given to the employee must be immediately surrendered, returned, or delivered to the security officer of the federal building.

3.1.6 Identification/Building Pass.

- a. The Contractor must make their personnel available for photo identification badges on a schedule to be determined by the COR. The badges will be made by the Government utilizing supplies, materials and equipment provided by the Government. Each Contractor employee must sign the appropriate badge at the time of photographing.
- b. The Contractor is responsible for ensuring that each of his/her employees performing work under this task order display their photo-identification badges at all times they are present on-duty in the building. Refusal or repeated neglect to display the photo-identification may result in an unsuitability determination.
- c. Upon termination, resignation or other event leading to a task order employee leaving duty under this task order, the Contractor is responsible for returning all Government identification, building passes, keys, and other Government property issued to that employee. Failure on the part of the Contractor may result in the Contractor's liability for all costs associated with correcting the resultant breach in building security. The Contractor must notify the COR when the employee badges are lost. It will be the responsibility of the Contractor to pay for replacement badges at the current replacement cost per badge.
- d. d) If applicable, the requirements of this clause are applicable to and must be flowed down to all subcontractors who will work at the Government (or name of client specific facility) facilities.

3.1.7 Hours of Work

Contractor personnel are expected to conform to normal operating hours. The normal core duty hours are 8:00 AM to 5:00 PM, Monday through Friday, with the exception of Federal Government holidays, with an allowance for a one-hour lunch period each day.

3.1.8 Productive Direct Labor Hours

The contractor can only charge the Government for "Productive Direct Labor Hours". "Productive Direct Labor Hours" are defined as those hours expended by Contractor personnel in performing work under this effort. This does not include sick leave, vacation, Government or contractor holidays, jury duty, military leave, or any other kind of administrative leave such as acts of God (i.e. hurricanes, snow storms, tornadoes, etc) Presidential funerals or any other unexpected government closures.

3.1.9 Government Holidays

The following Government holidays are normally observed by Government personnel: New Years Day, Martin Luther King’s Birthday, Presidential Inauguration Day (metropolitan DC area only), President’s Day, Memorial Day, Independence Day, Labor Day, Columbus Day, Veteran’s Day, Thanksgiving Day, Christmas Day, and any other day designated by Federal Statute, Executive Order, and/or Presidential Proclamation. Or any other kind of administrative leave such as acts of God (i.e. hurricanes, snow storms, tornadoes, etc) Presidential funerals or any other unexpected government closures.

3.2 Key Personnel

Key personnel for this effort are as identified below:

Name	Category
Richard J. Civetti	Program/Project Manager
Zeyno Aygen Dodd	Senior Database Administrator
Lynford Warner	Senior Application Software Engineer
Kevin Chung	Information Assurance Specialist

3.2.1 Key Personnel Definition.

Certain skilled experienced professional and/or technical personnel are essential for accomplishing the work to be performed. These individuals are defined as “Key Personnel” and are those persons whose resumes were submitted and marked by the vendor as “Key Personnel”. All staff proposed as KEY for this project must be full-time on this contract. No substitutions shall be made of accepted key personnel except for sudden illness or death, or termination of employment. Substitutions shall only be accepted if in compliance with “Substitution of Key Personnel” provision identified below.

3.2.2 Key Personnel Designation.

- a) For the purpose of the overall performance of this effort, the Contractor’s Project Manager shall be designated as a key person.
- b) The Project Manager shall be the Contractor’s authorized point of contact with the Government CO and the COR. The Project Manager shall be responsible for formulating and enforcing work standards, assigning schedules, reviewing work discrepancies, and communicating policies, purposes, and goals of the organization to subordinates.
- c) The Project Manager shall oversee the day-to-day activities of the project. The Project Manager shall be responsible for assigning ongoing tasks as they are received from the COTR, monitoring the work being performed to assure that tasks are completed on schedule, and validating all deliverables by performing several quality assurance checks before delivering those products to the COTR for final approval.
- d) The Project Manager or alternate must be available during normal duty hours, as specified herein and to meet with government personnel within 24 hours to discuss problems.

- e) The Contractor's Project Manager shall meet with the CO/COTR as necessary to maintain satisfactory performance and to resolve other issues pertaining to Government/Contractor procedures. At these meetings, a mutual effort will be made to resolve any and all problems identified. Written minutes of these meetings shall be prepared by the Contractor, signed by the Contractor's designated representative, and furnished to the Government within two (2) workdays of the subject meeting.
- f) The Project Manager and alternate or alternates must be able to read, write, speak, and understand English.

3.2.3 Key Personnel Substitution and/or Replacement.

All Contractor requests for approval of substitutions shall be submitted in writing to the COR at least twenty-five (25) calendar days in advance of the date on which a replacement must report for duty, and shall provide a reason for the need to replace someone, a complete resume for the proposed substitute, and any other information requested by the Contracting Officer necessary to approve or disapprove the proposed substitution. An interview may also be requested. The COR and the Contracting Officer will evaluate such requests and promptly notify the Contractor of approval or disapproval in writing.

3.3 Anticipated Travel.

Local and long-distance travel may be required. Accordingly, anticipated travel should be included in the contractor's cost proposal. All estimated travel will conform to the current Federal Travel Regulations (FTRs). After award, all travel shall receive government approval by the Contracting Officer's Technical Representative (COTR) prior to funds being expended. Travel expenses invoiced to the Government will be in accordance with FTR; expenditures that exceed the FTR will not be reimbursed by the Government. Currently the Government is estimating:

- Number of People required to travel: 2
- Destination (from/to) and Number of Trips
 - Washington, DC to Lenexa, KS 4
 - Washington, DC to Albuquerque, NM 2
 - Washington, DC to Aberdeen, SD 1
 - Washington, DC to Los Angeles, CA 1
 - Lenexa, KS to Muskogee, OK 2
- Number of Days
 - # Working days : 3
 - # Travel days 2
 - # Overnight nights 4

Example: Travel Monday, work Tuesday-Thursday, and return on Friday.

3.4 Place(s) of Performance.

Services may be provided off-site, on-site, or a combination of, depending on program requirements. However, the majority of the work will be performed at OHTA headquarters office, located in Washington, DC and the OHTA field office in Lenexa Kansas.

Office of Historical Trust Accounting

1801 Pennsylvania Avenue NW, Suite 500
Washington, DC 20006

Office of Historical Trust Accounting
17501 W. 98th Street, Suite 44-47
Lenexa, KS 66219

3.5 Period of Performance

The period of performance for this effort is date of award for a Base Period of one (1) year. This effort also includes four (4) option periods, which may be unilaterally exercised by the Government. Each option period shall not exceed one year in duration, unless mutually agreed upon and a formal modification issued. All terms and conditions applicable to the base period shall extend to the options unless otherwise agreed upon. The option period is subject to the availability of funds.

	Start Date	End Date
Base Year	12/23/2010	12/22/2011
Option Year 1	12/23/2011	12/22/2012
Option Year 2	12/23/2012	12/22/2013
Option Year 3	12/23/2013	12/22/2014
Option Year 4	12/23/2014	12/22/2015

3.6 Authority to Obligate the Government

The Contracting Officer is the only individual who can legally commit or obligate the Government to the expenditure of public funds. No cost chargeable to the proposed contract can be incurred before receipt of a fully executed contract or specific authorization from the Contracting Officer.

3.7 Quality Assurance

The COTR will review, for completeness, preliminary or draft documentation that the Contractor submits, and may return it to the Contractor for correction. Absence of any comments by the COTR will not relieve the Contractor of the responsibility for complying with the requirements of this work statement. Final approval and acceptance of documentation required herein shall be by letter of approval and acceptance by COTR. The Contractor shall not construe any letter of acknowledgment of receipt material as a waiver of review, or as an acknowledgment that the material is in conformance with this work statement. Any approval given during preparation of the documentation, or approval for shipment shall not guarantee the final acceptance of the completed documentation.

3.8 Contractor Interfaces

The Contractor and/or his subcontractors may be required as part of the performance of this effort to work with other Contractors working for the Government. Such other Contractors shall not direct this Contractor and/or their subcontractors in any manner. Also, this Contractor and/or their subcontractors shall not direct the work of other Contractors in any manner.

The Government shall establish an initial contact between the Contractor and other Contractors

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 51 of 82
--	-----------------------------------	--	---------------

and shall participate in an initial meeting at which the conventions for the scheduling and conduct of future meetings/contacts will be established. Any Contracting Officer's Technical Representatives (COTR) of other efforts shall be included in any establishment of conventions.

3.9 Materials and Property

3.9.1 Contractor Acquired Equipment, Supplies and Service

The contractor may be authorized by the government to procure goods and services needed in the performance of the work. Contractor shall request authorization from the COTR in advance of expending funds. The government maintains the right to supply the contractor with government furnished materials, supplies and services. ODC's may be required for this task. After award, all ODC's shall receive government COR approval prior to funds being expended. The contractor should include ODCs in their cost proposal to cover any costs associated with travel and/or other direct costs (ODC'S). ODC's are limited to \$3,000 on GSA schedule holders, unless the items are on the holder's schedule. In the event that ODC's are required over the \$3,000 threshold, and the items are not on the contractors schedule, the contractor will provide to the COR market analysis documentation for all items that are required to be procured, that have an extended price of \$3,000.00 or greater. Market analysis may consist of actual quotes received (3 minimum) or cost comparisons based on published price schedules such as those found on the GSA Advantage website. This information will be provided to the CO to make a final determination on procuring the item(s).

3.9.2 Government Furnished Equipment (GFE)

The contractor shall have full access to GFE and software to perform the duties on the project while performing duties in government space. Government shall furnish all office space, equipment, including both computer hardware and software, necessary for the contractor to perform the assigned work on-site, unless otherwise specified, to fully satisfy all operational requirements of this contract.

All Government Furnished Property referred to in this clause will remain the property of the Government, or its contractor, and under that entity's control at all times. The Government retains the right to withdraw or reallocate these resources at any time, and without notice, during the performance of this contract.

3.9.3 Government Furnished Information (GFI)

The contractor shall be furnished current task working papers, project descriptions, program briefing material and other pertinent information, and other documentation or material required to carry out the tasks described hereunder.

3.10 508 Standard Requirements

All electronic and information technology (EIT) must meet the applicable accessibility standards at 36 CFR 1194, unless an agency exception to this requirement exists. 36 CFR 1194 implements Section 508 of the Rehabilitation Act of 1973, as amended, and is viewable at <http://www.accessboard.gov/sec508/508standards.htm> - Part 1194.

The Standards apply to the following:

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 52 of 82
--	----------------------------	---	---------------

- Software Applications and Operating Systems
- Web-based Information or Applications
- Telecommunication Products
- Video and Multimedia Products
- Self Contained, Closed Products (e.g., Information Kiosks, Calculators, and Fax Machines)
- Desktop and Portable Computers

3.11 General Records Management for Records Generated in Executing the Contract

- a) Citations to pertinent laws, codes and regulations such as 44 U.S.C chapters 21, 29, 31 and 33; Freedom of Information Act (5 U.S.C. 552); Privacy Act (5 U.S.C. 552a); 36 CFR Part 1222 and Part 1228.
- b) Contractor shall treat all deliverables under the contract as the property of the Government for which the Government Agency shall have unlimited rights to use, dispose of, or disclose such data contained therein as it determines to be in the public interest.
- c) Contractor shall not create or maintain any records that are not specifically tied to or authorized by the contract using Government IT equipment and/or Government records.
- d) Contractor shall not use, sell, or disseminate copies of any deliverable that contains information covered by the Privacy Act of 1974 or that which is generally protected by the Freedom of Information Act.
- e) Contractor shall not create or maintain any records containing any Government records that are not specifically tied to or authorized by the contract.
- f) The Government owns the rights to the maximum extent practical to all data/records produced as part of this contract. (See Rights in Data-General, clause)
- g) The Government owns the rights to all electronic information (electronic data, electronic information systems, electronic databases, etc.) and all supporting documentation created as part of this contract.
- h) Contractor must deliver sufficient technical documentation with all data deliverables to permit the agency to use the data.
- i) Contractor agrees to comply with Federal and DOI records management policies, including those policies associated with the safeguarding of records covered by the Privacy Act of 1974. These policies include the preservation of all records created or received regardless of format (paper, electronic, etc.) or mode of transmission (e-mail, fax, etc.) or state of completion (draft, final, etc.).
- j) No disposition of documents will be allowed without the prior written consent of the CO. The Government and its Contractors are responsible for preventing the alienation or unauthorized destruction of records, including all forms of mutilation. Willful and unlawful destruction, damage

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 53 of 82
--	----------------------------	---	---------------

or alienation of Federal records is subject to the fines and penalties imposed by 18 USC 2701. Records may not be removed from the legal custody of the Agency or destroyed without regard to the provisions of the agency records schedules.

- k) Contractor is required to obtain the CO approval prior to engaging in any contractual relationship (subcontractor) in support of this contract requiring the disclosure of information, documentary material and/or records generated under, or relating to, this contract. The Contractor (and any subcontractor) is required to abide by Government and DOI guidance for protecting sensitive and proprietary information.

3.12 Administrative Considerations

3.12.1 Points of Contact

The Contracting Officer (CO) for this effort is as follows:

Department of the Interior
 Acquisition Services Directorate
 ATTN: Debra Hoffman, CO
 381 Elden Street, Suite 4000
 Herndon, Virginia 20170-4817
 Office: 703-964-3662; email Debra.Hoffman@aqd.nbc.gov

Contract Specialist for this effort is as follows:

Department of the Interior
 Acquisitions Services Directorate
 ATTN: Chris Sazama
 381 Elden Street, Suite 4000
 Herndon, VA 20170-4817
 Office: 703-964-3606; email Chris.Sazama@aqd.nbc.gov

3.13 Organizational Conflict of Interest

The effort to be performed by the contractor under this task order includes consultation and program management services. Consequently, performance of this task order creates potential organizational conflicts of interest such as are contemplated by Federal Acquisition Regulation (FAR) 9.505. It is the intention of the parties that the contractor will not engage in any other contractual or other activities which could create an organizational conflict of interest with its position under this task order; which might impair its ability to render unbiased advice and recommendations; or in which it may derive an unfair competitive advantage as a result of knowledge, information, and experience gained during the performance of this task order. The contractor shall not employ any person who is an employee of the United States Government if that employment would, or could appear to, cause a conflict of interest.

3.14 Payment for Unauthorized Work

No payments will be made for any unauthorized supplies and/or services or for any unauthorized

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 54 of 82
--	----------------------------	---	---------------

changes to the work specified herein. This includes any services performed by the Contractor of their own volition or at the request of an individual other than a duly appointed Contracting Officer. Only a duly appointed Contracting Officer is authorized to change the specifications, terms, and conditions under this effort.

3.15 Labor Category Descriptions

Project Manager

Minimum/General Experience: This position requires at least ten (10) years of combined IT experience that includes business and system requirements definition, system design, system development and/or system testing.

Functional Responsibility: Responsible for the overall management of the development tasks, and the Operation & Maintenance (O&M) activities. Supervises and directs staff on a daily basis. Experience in some project development life cycle phases from inception to deployment, with an ability to provide guidance and direction in these tasks areas is required. Defines and directs technical specifications and tasks to be performed by team members, defines target dates of tasks and subtasks. Directs completion of tasks within estimated timeframes and budget constraints. Schedules and assigns duties to subordinates and subcontractors and ensures assignments are completed as directed. Enforces work standards and reviews/resolves work discrepancies to ensure compliance with contract requirements. Reports in writing and orally to contractor management and Government Contracting Officer's Technical Representative (COTR). Provides competent leadership and responsible program direction through successful performance of a variety of detailed, diverse elements of project transitioning. Plans and directs technological improvements and project management implementation. Manages a diverse group of functional activities, subordinate groups of technical and administrative personnel. Provides business, technical, and personnel management across multiple projects, such as engineering studies, computer applications and systems development.

Ensures compliance with contract requirements. May be a senior technical expert who provides advice, design, and development on complex technical tasks. Leads software projects on a variety of software platforms. Skills should include cost and budget management, risk management, resource management and very strong customer interfacing abilities. Must be strong at creating and verifying software project documentation including systems requirements, systems designs, test plans, and project reviews. Works independently without direct supervision. Must possess strong written and oral communication skills to ensure effective interaction with customers and project team members. Management of help desks; knowledge of PC operating systems, applications, and networks; and supervision of help desk personnel.

Minimum/General Experience: A Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline.

Senior Database Administrator

Minimum/General Experience: Six (6)+ years of devoted experience with designing, developing, configuring and maintaining MS SQL Server and databases. Extensive expertise in Installing, Configuring, and Administering Microsoft SQL Server Enterprise Editions. Designing and Implementing Databases with Microsoft SQL Server Enterprise Editions. Experience and knowledge of database security architecture, performance tuning, capacity planning, and disaster recovery processes and procedures. Proven experience with complex database systems migration, consolidation, and integration.

Functional Responsibility: Configure, administer, maintain and support an array of Enterprise Microsoft SQL Servers in production, test and dev environments. Develop, implement, and enforce policies and procedures to ensure the security and integrity of corporate databases. Maintain enterprise databases and database servers in production, test and development environments. Monitor database performance and tune database management system as necessary. Work closely with system administrators during software installation and upgrades on Microsoft SQL Server. Offer assistance to developers in tuning database queries under development.

Minimum Education: Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or other related discipline and MCDBA certified.

Senior Application/Software Engineer

Minimum/General Experience: Microsoft or Industry Certified Professional. Ten (10) years experience (or equivalent combination of education and experience). Relevant experience includes, but is not limited to, use of programming languages, knowledge of database management systems, and software development management experience.

Functional Responsibility: Conducts or participates in the research, design and development of systems software, software applications and/or tools for new programs and subprograms as well as enhancements, modifications and corrections to existing software. Codes, tests, integrate and documents software solutions. May also design, develop and implement database, Internet/Web-based applications, personal computer/client server support, systems programming, applications design and development, database design and administration, telecommunications and network support and administration to accommodate a variety of user needs. Acts as lead developer/team leader in Visual Basic, Access, Visual C++, or Internet/Intranet development typically in concert with a Microsoft Back Office Environment. Assumes primary responsibility for application design and development; consults with clients to determine needs and meets with clients on an on-going basis throughout application development. Coordinates with the Project and/or Program Manager to ensure problem solution and user satisfaction. Prepares milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives.

Minimum Education: A Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. With a Master's Degree (in the fields described above); eight (8) years general experience of which at least two (2) years must be specialized experience is required.

Application/Software Engineer

Minimum/General Experience: Microsoft or Industry Certified Professional. Ten (10) years experience (or equivalent combination of education and experience). Relevant experience includes, but is not limited to, Visual Basic, Access, Visual C++, or Internet/Intranet development typically in concert with a Microsoft Back Office Environment.

Functional Responsibility: Participates in the design and development of systems software, software applications and/or tools for new programs and subprograms as well as enhancements, modifications and corrections to existing software. Codes, tests, integrate and documents software solutions. May also design, develop and implement database, Internet/Web-based applications, personal computer/client server support, systems programming, applications design and development, database design and administration, telecommunications and network support and administration to accommodate a variety of user needs. Duties may include designing, programming, documenting, and implementing software applications.

Minimum Education: A Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. With a Master's Degree (in the fields described above); four years general experience of which at least two years must be specialized experience is required.

Internet/Intranet Developer

Minimum/General Experience: Minimum 3 years of software development experience coding C# and VB.NET, developing and maintaining SharePoint sites, supporting and working with MOSS 2007 and SharePoint 3.0, using Visual Studio and SharePoint Designer. The candidate should also have strong experience writing stored procedures, creating tables/views/etc. in SQL Server 2005. Experience with Microsoft Reporting Services will be an added advantage.

Functional Responsibilities: Works closely with Project Manager or lead Application/Software Engineer to design, develop, debug, implement and troubleshoot software code (i.e., HTML, CGI, and JavaScript) for components of Internet/Intranet applications and the Design, develop, and implement SharePoint portal for backoffice applications. Works with members of a project team to develop the site concept, interface design, and architecture of the website. Responsible for interface implementation.

Minimum Education: A Bachelor's Degree in Computer Science, Information Systems, Engineering, Business, or other related scientific or technical discipline. 5-10 years programming experience with emphasis on SharePoint server experience (SharePoint programming is required), c++, C#, as well as experience in workflow design.

Quality Assurance Analyst

Minimum/General Experience: software development discipline, Configuration Management, verification and validation, software testing and integration, software metrics, and their application to software quality assessment. General experience includes increasing responsibilities in quality assurance, quality control, and team leader responsibilities.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 57 of 82
--	----------------------------	---	---------------

Functional Responsibility: Maintains the level of quality throughout the software life cycle. Conducts formal and informal reviews, at predetermined times, throughout the development life cycle. Provide technical and administrative guidance for personnel performing development tasks, including review of work products for accuracy, adherence to the design concept and to applicable standards, review of program documentation to assure compliance with government standards/requirements, and for progress in accordance with schedules. Coordinate problem solution and user satisfaction. Make recommendations, if needed, for approval of major system installations. Prepare milestone status reports and deliveries/presentations on the system concept to colleagues, subordinates, and end user representatives. Establish and maintain a process for evaluating software and associated documentation. Determines the resources required for quality control.

Minimum Education: A Bachelor's degree in Computer Science, Information Systems, Engineering, Business, or other related discipline. With a Master's Degree (in the fields described above), 6 years of general experience of which at least 4 years must be specialized experience.

Information Assurance (IA) Specialist

Minimum/General Experience: Experience with security programs, policy development, security life cycle management, and security risk assessment. Responsible for providing technical and security policy for the protection of automated information systems including Internet/Intranet systems. Develop security documentation, including security plans, configuration management plans, and contingency plans in compliance with IA policy. Develop verification procedures for executing risk assessments and security test and evaluations, and conduct risk assessments to ensure that systems are operating securely. Designs, develops, engineers, and implements solutions to various security requirements including firewalls, threat assessment, vulnerability assessment, risk assessment, etc. Experienced in implementing Intrusion Detection Systems, Public Key Infrastructure, and preparing security related documentation for all phases of Security Life Cycle Management.

Functional Responsibility: Provide technical analysis, make recommendations, and implement approaches to solving security problems associated with network access controls, user authentication, and authorization.

Minimum Education & Experience: Bachelor's Degree in related field or equivalent. Five (5) years of general experience is considered equivalent to a Bachelor s Degree or four (4) years of general experience and a technical certification such as a MCSE, CNE, or CCIE is considered equivalent to a Bachelors Degree.

Senior Systems Administrator

Minimum/General Experience: 8+ years of managing a Windows Server environment (Windows 2003 Server required) (2008 is a plus). extensive knowledge and understand how the servers operates and know how to maintain the computer system, install software and patches, resolve problems, maintain data files, monitor the system, and execute systems backup and recovery. Expertise of Microsoft based systems to include operating Systems and server applications (MS Exchange 2003/2007, AD 2003/2008, DNS, Print/File services). Strong Hands on Active Directory skills required, preferably with experience managing complex, multi-domain forests and

	Document No. D11PDI8655	Document Title OHTA- IT Support Services	Page 58 of 82
--	----------------------------	---	---------------

trusts. Server management experience desired, especially with an emphasis on Dell and IBM Servers.

Functional Description: Provides expertise to properly maintain IT systems operations, monitoring application/system software and hardware operations, routine/high priority system problem identification, and high priority corrective action. Coordinates system resource availability with database analysts, system and application programmers, and other users. Performs/oversees systems administration and network management/administration responsibilities. Ensures compliance with electronic and physical security procedures and standards. Provides continuous liaison with users and project staff to identify unique and/or common difficulties and prepare plans for their resolution. Provides assistance to users in accessing and using business systems.

Minimum Education: Requires a Bachelor's degree and five (5) years of progressively more responsible experience performing systems and network management/administration responsibilities. Microsoft Certified Systems Administrator (MCSA) and Microsoft Certified Systems Engineer (MCSE) credentials.

Systems Administrator

Minimum/General Experience: 3+ years of managing a Windows Server environment (Windows 2003 Server required) (2008 is a plus). Knowledge and understand how the servers operates and know how to maintain the computer system, install software and patches, resolve problems, maintain data files, monitor the system, and execute systems backup and recovery. Expertise of Microsoft based systems to include operating Systems and server applications (MS Exchange 2003/2007, AD 2003/2008, DNS, Print/File services). Server management experience desired, especially with an emphasis on Dell and IBM Servers. Coordinates system resource availability with database analysts, system and application programmers, and other users. Performs systems administration and network management/ administration, and system help desk responsibilities.

Functional Description: Provides expertise to properly maintain IT systems operations, monitoring application/system software and hardware operations, routine/high priority system problem identification, and high priority corrective action. Coordinates system resource availability with database analysts, system and application programmers, and other users. Performs/oversees systems administration and network management/administration responsibilities. Ensures compliance with electronic and physical security procedures and standards. Directs and trains users. Provides continuous liaison with users and project staff to identify unique and/or common difficulties and prepare plans for their resolution. Provides assistance to users in accessing and using business systems.

Minimum Education: An Associate's Degree in Computer Science, Information Systems, Engineering, and A+ certification and Network+ certification is required. Specialized help desk experience of six (6) years may be considered as equivalent qualification in lieu of an Associate's degree. Microsoft Certified Systems Administrator (MCSA) credentials are desired.

Technician/ Help Desk Specialist

Minimum/General Experience: Four years of help desk/user support experience. Have a strong background in PC troubleshooting, PC assembly, operating system and application software installation.

	Document No. D11PD18655	Document Title OHTA- IT Support Services	Page 59 of 82
--	-----------------------------------	--	---------------

Functional Responsibility: Provides phone and in-person support to users in the areas of e-mail, directories, standard Windows desktop applications, and applications developed under this contract or predecessors. Diagnoses and resolves complex network configuration, design and PC hardware/ software problems. Serve as a technical point of contact for troubleshooting hardware/software PC and printer problems.

Minimum Education: An Associate's Degree in Computer Science, Information Systems, Engineering, and A+ certification and Network+ certification is required. Specialized help desk experience of six (6) years may be considered as equivalent qualification in lieu of an Associate's degree.

Program Administration Assistant

Minimum/General Experience: Experienced in office administration and developing technical presentations for publications and documents. Experience in using automated word processing, graphics systems, and spreadsheet applications. Specialized experience includes: preparing technical documentation, which is to include researching for applicable Government and industry documentation standards. General experience includes technical writing and documentation experience pertaining to all aspects of ADP. Demonstrated ability to work independently or under only general direction.

Functional Responsibility: Directly supports the Program Manager by maintaining files, prepares correspondence, schedules, and coordinates travel. Duties may include assisting in the preparation of management and financial reports, presentation graphics, and support the development of contract deliverables and reports. Responsible for integrating the graphics generated with automated tools and the deliverable documents.

Minimum Education: Associate's degree (in the fields described in this paragraph). With a Bachelor's degree (in the fields described above), 2 years of general experience of which at least 1 year must be specialized experience. With 6 years of general experience of which at least 4 years is specialized, a degree is not required.