NAVFAC
ENTERPRISE HOSTING SERVICES
(EHS)
PERFORMANCE WORK STATEMENT
(PWS)

VERSION 3

8/26/2011

EHS PWS

Table of Contents

1. General/Organization/Scope/Background/Objective 4
1.1. Organization to be supported: 4
1.2. Scope: 4
1.2.1. Clearances and Licensing: 6
1.2.2. Privacy Act: 7
1.2.3. Access Requirements: 7
1.3. Background: 8
1.4. Objective: 8
2. Definitions as applied to this contract 9
2.1. Common Operating Environment (COE) 9
2.2. Technology Stacks (TS) 9
2.3. Technology Refresh (TR) 9
2.4. Sustainment and Maintenance 9
2.5. Emerging Systems 9
2.6. Large Hosting Projects 9
2.7. Continuous Process Improvement (CPI) 10
2.8. Government-Approved Outages 10
2.9. Application Virtualization 10
2.10. Hardware Virtualization 10
2.11. Storage Virtualization and Consolidation 10
2.12. Deliverables 11
2.13. Knowledge and Skill Levels 11
2.14. Acronyms 11
3. Enterprise Hosting Services (EHS) Contract Description And Deliverables 15
3.1. Hosting Infrastructure Operations, Sustainment, and Maintenance Support 19
3.1.1 Server Administration 19
3.1.1.a Server build and configuration 19
3.1.1.b Software Installations, Updates and Configuration 20
3.1.2 Enterprise Storage Administration 22
3.1.2.a Enterprise Storage Configuration 22
3.1.2.b Storage Allocation 23
3.1.3 Backup Administration 24
3.1.3.a Backup Device Configuration 24
3.1.3.b Backup jobs management 24
3.1.4 Networking and inter-connectivity 25
3.1.5 Optimization and Performance Tuning 26
3.1.6 Software and Hardware Maintenance Support 27
3.1.7 Hardware Refresh 28
3.2. Enterprise Database Operations, Sustainment, and Maintenance 29
3.2.1. Database Systems Administration 29
3.2.1.a Database Software Installation and Configuration. 29
3.2.1.b Database and Instance Creation and Configuration 30
3.2.1.c Database Monitoring, Optimization and Tuning 31
3.2.1.d Database Backup and Restoration. 32
3.2.1.e Database Sustainment and Maintenance. 33
3.3 Applications Technology Stack Operations, Sustainment, and Maintenance 34
3.3.1 COTS/GOTS Systems Administration 34
3.3.1.a COTS/GOTS Software Component Updates and Configuration 34
3.3.2 Business Systems and Web Sites Administration 36
3.3.2.a Systems Integration, Interface, connectivity, User Access 36
3.3.2.b Applications Sustainment and Maintenance 37
3.3.3 Performance Monitoring, Optimization and Tuning 38
3.4 Incident Response, Service Request Fulfillment and Tracking 39
3.4.1 Service Request Fulfillment 39

EHS PWS

3.4.2 Incident Response and Call-Back Support ... 39
3.5 Security Scans, Fixes, Mitigation Actions and Tracking ... 41
3.6 Standardization, Continuous Process Improvement, and Documentation ... 42
3.7 Emerging Systems, Large Projects, and Emerging Technology Support ... 43
3.7.1 System Requirements Review ... 43
3.7.2 Technological Analysis and Design ... 43
3.7.3 Execution and Status Tracking and Reporting ... 44
3.7.4 Deployment, Training and Closeout ... 44
3.8 Contract Management ... 45
3.9 Performance Requirements Summary Matrix ... 46
3.10 Deliverables ... 67
4. Quality Planning, Control And Assurance ... 69
5. Government Furnished Information, Services, And Equipment ... 69
6. Contractor Furnished Information, Services, And Equipment ... 70
7. Other Information/Period Of Performance/Travel/ Points Of Contact ... 70
7.1. Hours of Work: ... 70
7.2. Place of Performance: ... 70
7.3. Period of Performance: ... 70
7.4. Travel: ... 71
7.4.1. Air: ... 71
7.4.2. Non-Reimbursable Travel: ... 71
7.5. Training: ... 71
7.6. Monthly Status Reports: ... 71
7.7. NAVFAC IT Hosting Architecture: ... 71
7.8. Key Positions: ... 71
7.9. Contractor Identification: ... 72
7.10. Intellectual Property: ... 72
7.11. Transition between Contract and Continuity of Service: ... 72
8. Attachments ... 74
Attachment 01 - Enterprise Business Systems ... 74
Attachment 02 - Common Operating Environment (COE) ... 75
Attachment 03 - Application Technology Stacks and Hosting Services ... 76
Attachment 04 - Key Positions ... 77
Attachment 05 - Non Disclosure Form ... 78
Attachment 06 - Department of Homeland Security Employment Eligibility Verification, Form I-9 ... 79
Attachment 07 - Contractor Verification System (CVS) ... 80
Attachment 08 - System Authorization Access Request Form (SAAR) ... 81

EHS PWS

1. General/Organization/Scope/Background/Objective

1.1. Organization to be supported:

Navy Facilities Engineering Command
1322 Patterson Ave SE
Washington Navy Yard, DC 20374-5065

Work is to be accomplished for the Naval Facilities Engineering Command (NAVFAC) Command Information Officer (CIO).

The recurring phrase, "The contractor shall," means that the firm selected for this procurement will, in accordance with all applicable Federal, state, and local laws, regulations, guidance, and policies, furnish the necessary personnel, services, products, materials, equipment, knowledge, and expertise to successfully complete the tasks required under this Contract.

The Contractor shall be responsible for complying with all applicable Federal Acquisition Regulations (FAR), and Defense Federal Acquisition Regulations (DFAR).

1.2. Scope:

Naval Facilities Engineering Command (NAVFAC) has a requirement to host an array of Enterprise Business Systems that will be utilized throughout various Navy Organizations to include all NAVFAC sites, all Navy Regions, the Marine Corps, and select private business partners. This array of Enterprise Business Systems supports the broad spectrum of NAVFAC's business, employs a broad range of technical solutions, and could vary from a web-based application to a client server- & web-based application to a data warehouse that supports NAVFAC corporate reporting. Client server applications are accessed via thin client, i.e. Citrix protocols. The list of enterprise-wide business systems are listed in the Business System Overviews (Attachment 01).

As a result, NAVFAC has a need for technological support for the day-to-day operations, sustainment and maintenance of the hosting infrastructure in a secured environment. This includes: systems administration of all servers, storage, internal network infrastructure, systems integration and interconnectivity, applications technology stacks, enterprise databases, enterprise business systems administration, hosting services, user accessibility, systems security, change andconfiguration management. Attachment 02, NAVFAC Common Operating Environment (COE), describes the existing environments, network boundaries, zones, servers, and storage platforms that comprise the NAVFAC Data Center hosting infrastructure located at NAVFAC Information Technology Center (NITC), Port Hueneme, California. Attachment 01 lists the NAVFAC Enterprise Business Systems that are hosted within the NAVFAC Data Center hosting facility.

The NAVFAC Data Center hosting environments consists of two accredited network environments. Changes to the hosting environments are subject to NAVFAC Information Technology Center(NITC) Operations Control Board (OCB) approval prior to implementation. Hosting environments are:

- DEVCOI contains the Experimental, Development, Test and Staging regions. This is where application developers develop and test their codes. The NAVFAC Application

HHS PWS

Service Provider (NASP) technical subject matter experts (SMEs) also use this environment to test new software, patches, and security fixes.

- EDMZ contains the Acceptance and Production regions. This also includes the remote Continuity of Operation and Disaster Recovery site. Before any change is applied to the EDMZ infrastructure or business systems hosted therein, they must first be successfully tested in non-production regions.

When technology reach end of life and new technologies become available, the NAVFAC Data Center hosting facility is required to perform technology refreshes on its hosting infrastructure. Technology refresh projects could range from hardware upgrades to application software version/release upgrades. The NAVFAC Data Center hosting facility performs hardware refresh and software upgrades once per year.

As existing Business Systems undergo life-cycle revision, or as new Business Systems are approved for hosting at the NAVFAC Data Center hosting facility, additional servers, storage, and skill sets may be required . An average of two new business systems per year may be brought up online or undergo major revision or upgrade to another software or technology stack.

To ensure continuity of operations during natural disasters and/or calamities, the NAVFAC Data Center hosting facility remotely maintains servers, operating systems and storage devices located at the Continuity of Operation and Disaster Recovery (COOP/DR) site in Norfolk, Virgina. Disaster recovery testing is scheduled by the Information Assurance team and executed by the NAVFAC Application Service Provider (NASP) technical staff.

IT systems security implementation is a major factor in keeping the "Authority to Operate (ATO)" not just for the hosting environments but is also required for each individual business systems hosted at the NAVFAC Data Center. The Federal Information Security Management Act (FISMA) shall be continuously reviewed and complied with. Each business systems listed in Attachment 01 undergo FISMA review or re-accreditation once per year. In collaboration with the Information Assurance Team, Central Design Agency (CDA) and the NASP technical SMEs, the Contractor shall determine the best approach for meeting IA and FISMA compliance without impacting business systems availability and performance.

The Contractor complements the government workforce in maintaining the day-to-day operations, maintenance and sustainment of the overarching NAVFAC Data Center hosting environments mentioned above, ensuring all hosting infrastructure listed in Attachment 02 - Common Operating Environment (COE) are maintained, and all hosting services identified in the Attachment 03 - Technology Stacks and Hosting Services are functioning and available to support business systems hosted therein. This includes maintaining the security posture across all hosting environments, and complying with established NITC standard business processes (example: change management, configuration management, portfolio management).

The Contractor shall provide surge personnel requirements to meet the needs for large hosting projects. "Large hosting projects" is defined in Section 2.6 of this contract.

This is a Performance Work Statement (PWS). The scope of this PWS is to provide:

- Recurring support for day-to-day technical, operational, sustainment, maintenance, and monitoring of the overarching NAVFAC hosting infrastructure to include: servers, storage, operating systems, backups, applications technology stacks, internal network infrastructure; systems integration; internal network connectivity; cabling; IAV and STIG security fixes; one-off patches and software component release updates; system change and configuration tracking; service fulfillment requests; troubleshooting; continuous process improvements, and documentation. For continuity of service in fulfilling these requirements, the Contractor shall

FISPWS

provide, at a minimum, full time equivalent (FTEs) employees for positions identified in Attachment 04 - Key Positions.

- Large hosting projects support for surge requirements needing more than 120 billable hours of effort. Large projects and skill types are defined in Section 2.6 of this contract.

The Contractor shall provide personnel, materials, equipment and transportation necessary (except as otherwise specified) to accomplish the requirements of this Contract.

1.2.1. Clearances and Licensing:

Contractor personnel working on this task shall be U.S. Citizens.

All tasks required in this Contract are IAT Level II "Privileged Access" in accordance with SECNAV M-5510.30 (e.g. involving super user or root access, direct access to operating system level functions, access to change control parameters of routers, multiplexers, and other key information system/network equipment or software; ability and authority to control and change program files, and other users' access to data or equivalent access) . Appropriate background check levels should be at the National Agency Check with Local Agency Check and Credit Check (NACLC) or higher level for all resources provided in support of this contract.

Work performed as part of executing this requirement will be at the SENSITIVE BUT UNCLASSIFIED. The contractor shall pursue and obtain final appropriate clearances (as defined by SECNAV M5510.30 at https://doni.daps.dla.mil/SECNAV%20Manuals1/5510.30.pdf - see sections 6-8 paragraph j.) for all personnel as required by individual task. All contractor personnel shall have a successfully adjudicated Access National Agency Check with Inquiries (ANACI) or National Agency Check with Local Agency (NACLA) as required by Information Technology (IT) level II "Limited Privileged Access. This shall also apply to all sub-contractor personnel.

The contractor shall establish and maintain an access list of those employees working on this Contract. A copy of the access list shall be furnished to the Command Information Assurance Manager (CIAM). All personnel reassignments and changes shall be documented within 3 business days via a revised access list provided to the NAVFAC CIAM. NAVFAC will provide the contractor access to all areas as necessary to support this effort.

Specific tasks may require specialized certifications as identified in the performance work statement.

The Contractor shall ensure that personnel accessing information systems have the proper and current information assurance certification to perform information assurance functions in accordance with DoD 8570.01-M, Information Assurance Workforce Improvement Program, and SECNAV M-5239.2 Department of the Navy Information Assurance (IA) Workforce Management Manual. The Contractor shall meet the applicable information assurance certification requirements, including:

(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M; and

(2) Appropriate operating system certification for information assurance technical positions as required by DoD 8570.01-M.

FFS PWS

Upon request by the Government, the Contractor shall provide documentation supporting the information assurance certification status of personnel performing information assurance functions.

Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions.

SECNAV M-5239.2 (Appendix G - OS Commercial Certification) lists special certification requirements applicable for this Contract. The contractor shall adhere to any modifications to the SECNAV M-5239.2 as they become available.

The contractor shall maintain and keep up-to-date their employee IA certification, and shall pay for all training, training travel, study time, exam and certification/re-certification.

1.2.2. Privacy Act:

Work on this project requires that Contractor personnel have access to Privacy Information to legally support Business Systems hosted at NITC. Personnel shall adhere to the Privacy Act, Title 5 of the U.S. Code (USC), Section 552a and applicable agency rules and regulations.

Contractor will be held liable for all data breaches where he/she is determined to be culpable (e.g., contract proprietary information, social security numbers (SSN) and other sensitive personnel information, etc). Contractor will be held liable and will be required to take steps such as notifying affected parties or providing credit monitoring.

Contractor personnel shall sign a Non-Disclosure Form (Attachment 05).

1.2.3. Access Requirements:

Contractor employees shall fill out a Department of Homeland Security Employment Eligibility Verification, Form I-9 (Attachment 06).

Contractor personnel shall coordinate with the Government sponsor to complete and submit an application for a DOD Common Access Card (CAC) through the Contractor Verification System (CVS), see Attachment 07 for the application procedures. The issuance of a Common Access Card (CAC) to a contractor requires, at a minimum, a completed National Agency Check (NAC), or what's considered a trustworthiness check, as well as an initiated National Agency Check with Written Inquiries (NACI). Companies who employ government contractor personnel will have to complete and submit the NACI on behalf of the individual prior to their arrival on-site. Contractor shall complete and submit a NACI on behalf of their employees prior to arrival on-site. This policy is in accordance with the DoD Physical Security Program, DOD 5200.8-R and the Contractor Verification System (CVS) Trusted Agent program.

Once the CAC request has been approved, Contractor personnel will proceed to the designated CAC issuance location identified by the Government sponsor with the appropriate documentation to support their identification and/or citizenship. The CAC issuance location will then issue the CAC.

Contractor employees traveling overseas must be eligible to obtain a passport.

Contractor employees shall successfully complete an online Information Assurance (IA) training class (approximately 1.5 hours in duration) each year.

EHS PWS

Contractor employees shall fill out a System Authorization Access Request Form (SAAR) to obtain access to any Government system (remote or otherwise), see Attachment 08

Within 7 working days of termination, the contractor shall adhere to NAVFAC checkout procedures for the termination and/or collection of all Public Key Infrastructure (PKI), CAC, NAVFAC Badges, Parking Passes, and Parking Decals. This pertains to NAVFAC support contractors both on site and off site.

1.3. Background:

The Naval Facilities Engineering Command (NAVFAC) is an Echelon II Systems Command under the Chief of Naval Operations (CNO), with additional authorities and responsibilities from the Secretary of the Navy (SECNAV). NAVFAC is a global military command with a Headquarters element and Component Commands that work together as one organizational team. NAVFAC also provides technical support for Navy expeditionary engineer readiness and doctrine, and program management support for multiple NAVFAC/CEC/SEABEE programs, including the Ocean Facilities Program and the Sealift Support Program.

The Naval Facilities Engineering Command (NAVFAC), Command Information Officer (CIO) has a requirement to provide optimized IT services to a global footprint of internal and external customers. Today, NAVFAC IT application hosting services is provided by one (1) Omnibus contract. This Contact is sub-divided into functional categories:

- Enterprise Database Sustainment and Maintenance Support
- Hardware and Internal Network Sustainment and Maintenance Support
- Applications and Technology Stack Sustainment and Maintenance Support
- Emerging Systems and Large Hosting Projects Support

Contractor support services will primarily be at NAVFAC's Information Technology Center (NITC), Port Hueneme, California. Some may be provided at various NAVFAC activities, as appropriate. This acquisition is one (1) of four (4) major acquisitions that will encompass all contractor-provided IT services for NAVFAC. The other three Omnibus Contracts in place for NAVFAC are Enterprise Business Support - Commercial off the Shelf(EBS-COTS), Enterprise Business Support - Non Commercial off the Shelf(EBS-NonCOTS)and EOS (Enterprise Operations Support).

1.4. Objective:

The objectives of this acquisition is to provide IT services support to the NITC hosting infrastructure on a 24x7x365 basis required to effectively and efficiently sustain all hosting services, operating systems, servers, storage devices, databases, technology stacks, and network components that support the usability and availability of business systems hosted therein. These IT services support type include:

- Routine and recurring sustainment support for day-to-day operations, sustainment, monitoring and maintenance of existing hardware, parts replacements, applications services, operating systems, utility software, internal network, system integration and interconnectivity, internal network management, troubleshooting, system availability monitoring, performance optimization, systems tuning and configuration, security compliance and mitigations, service request fulfillment, software patches, system change and configuration implementation and tracking, continuous process improvement and

EIS PWS

procedure documentation. This include off-hour call-back support and weekend maintenance support.

- Surge personnel support for large hosting projects requiring more than 120 billable hours of effort. Large hosting projects is defined in Section 2.6 of this contract.

2. Definitions as applied to this contract

2.1. Common Operating Environment (COE)

The Common Operating Environment (COE) identifies the layers of the NAVFAC Enterprise hosting infrastructure, network boundaries/Zones, and the hardware/software/storage platform. Attachment (02) is a representation of the NAVFAC/NITC Data Center COE.

2.2. Technology Stacks (TS)

The NITC enterprise applications hosting architecture supports distinct and separate technology stacks based on application requirements, but are inter-related and inter-dependent with each other. Attachment 03 - Technology Stacks and Hosting Services provides a description of the various technologies used to support applications and hosting services offered at the NAVFAC Data Center.

2.3. Technology Refresh (TR)

NITC performs periodic replacement of equipment to ensure continuing reliability of equipment and/or improved speed and capacity. To meet IT roadmaps for consolidation and refresh requirements, NITC must be able to change rapidly without substantially impacting or reducing capability enhancements that are coordinated in obsolete solutions. Major technology refresh requiring re-designing the hosting architecture to better meet technology roadmaps (ie: virtualization, consolidation, cloud computing), is a viable option for NITC if it meets DOD initiative for server footprint reduction.

2.4. Sustainment and Maintenance

NITC performs routine and recurring day-to-day operational sustainment and technical support of all hosting services and applications hosted at the NITC hosting center. Maintenance work is normally performed during non-core hours and weekends to minimize impact to the user community. Sustainment and maintenance tasks are tracked through the NITC change management process.

2.5. Emerging Systems

NITC maintains a common operating environment (COE) and core technology stack. New systems that do not conform to the existing NITC hosting COE or Technology Stacks, and require separate server environment, are considered "emerging" systems. Once the system is fully deployed, it becomes part of the COE and/or technology stack, and shall require daily sustainment and maintenance support. Government estimates two (2) occurences of emerging systems within the life of this contract.

2.6. Large Hosting Projects

These are large scale hosting projects that require more than 120 billable hours of effort. These require a pool of subject matter experts which include: architects, engineers, project managers, vendor-specific consultants and technical SMEs. The 120 billable hours shall not include wait-time for other actions which include: IA accreditation, commodity acquisition, NMCI network decision meetings, and software portfolio update. Large hosting projects can include:

EHS PWS

- Converting and migrating from legacy systems
- Major hardware refreshes
- Technology stack or COTS version upgrades
- Establishing new hosting service platforms
- Emerging technologies and delivery techniques
- New software deployments
- New business system hosting support

2.7. Continuous Process Improvement (CPI)

The NITC hosting center maintains processes and procedures for standardization. These processes and procedures are based on CMMI and ITIL framework and industry's best practices. Government-initiated audits are conducted to ensure these processes and procedures are followed and maintained. All employees of the hosting facility (both government and contractors) shall comply with established processes and continually update SOPs within their area of responsibility.

2.8. Government-Approved Outages

The NITC maintains a calendar of approved maintenance schedules that require system outages. These are usually done during non-core hours and weekends in response to warning messages and system alerts that can eventually lead to major system crashes . Government-approved outages include: (1) scheduled weekend maintenance, (2) scheduled system maintenance during the week due to system issues/failures, and (3) critical IA/IAVA/INFOCON/SRR implementations which could happen during the week.

2.9. Application Virtualization

Application Virtualization describes technologies that improve portability, manageability and compatibility of applications by encapsulating them from the underlying operating system on which they are executed. A fully virtualized application is not installed in the traditional sense, although it is still executed as if it were. The application is fooled at runtime into believing that it is directly interfacing with the original operating system and all the resources managed by it, when in reality it is not. In this context, the term "virtualization" refers to the artifact being encapsulated (application), which is quite different to its meaning in hardware virtualization, where it refers to the artifact being abstracted (physical hardware). CDA (for GOTS) and software vendor (for COTS) support must be obtained prior to implementation in the NITC hosting environments.

2.10. Hardware Virtualization

Hardware virtualization is a virtualization of computers or operating systems. It hides the physical characteristics of a computing platform from users, instead showing another abstract computing platform. NITC is using VMWare and Solaris Container Virtualization Software to control virtualization. Hardware and operating systems virtualization is an on-going effort at the NAVFAC Data Center hosting facility to comply with DON's server footprint reduction initiative.

2.11. Storage Virtualization and Consolidation

Storage virtualization is the pooling of physical storage from multiple network storage devices into what appears to be a single storage device that is managed from a central console. NITC uses NetApp to control storage from EMC and NetApp

Storage consolidation is an ongoing effort at NITC to standardize and consolidate storage needs on the NetApp SAN System.

EITS PWS

2.12. Deliverables

Contract Deliverables: Deliverables starting with the letter "C". These are core contractual deliverables with required completion dates, and are integral to the successful delivery of the hosting contract. Examples include but not limited to: key positions are occupied with fully qualified personnel, large projects are successfully completed as scheduled. Incentives may be offered for early completion without incurring additional cost to the government.

Performance Deliverables: Deliverables starting with the letter "P". These are compliance requirements that shall be met by all personnel (government and contractors) in the hosting facility to ensure all NITC standard business processes are complied with. Examples include but not limited to: use of checklists to ensure system change and configuration changes are tracked; SOPs are properly maintained for continuous process improvement. Incentives may be offered for excellent services provided for maintaining high availability and high performing systems.

2.13. Knowledge and Skill Levels

Entry-Level: Applies fundamental concepts, processes, practices, and procedures on technical assignments. Performs work that requires practical experience and training. Work is performed under supervision.

Journeyman: Possesses and applies expertise on multiple complex work assignments. Assignments may be broad in nature, requiring originality and innovation in determining how to accomplish tasks. Operates with appreciable latitude in developing methodology and presenting solutions to problems. Contributes to deliverables and performance metrics where applicable.

Senior: Possesses and applies a comprehensive knowledge across key tasks and high impact assignments. Plans and leads major technology assignments. Evaluates performance results and recommends major changes affecting short-term project growth and success. Functions as a technical expert across multiple project assignments. May supervise others.

Master: Provides technical/management leadership on major tasks or technology assignments. Establishes goals and plans that meet project objectives. Has domain and expert technical knowledge. Directs and controls activities for a client, having overall responsibility for financial management, methods, and staffing to ensure that technical requirements are met. Interactions involve client negotiations and interfacing with senior management. Decision making and domain knowledge may have a critical impact on overall project implementation. May supervise others.

2.14. Acronyms

- ACNO-IT - Assistant Chief of Naval Operations for Information Technology
- ACTR – Assistant Contract Technical Representative (NMCI Term)
- AHF – Application Hosting Facility
- ANACI – Access National Agency Check with Inquires
- AQL –Acceptable Quality Level
- ASDP – Abbreviated Systems Decision Paper
- ASP – Active Server Page?
- ATL – Automated Tape Library
- B2B – Business to Business
- BCA – Business Case Analysis
- BCP – Business Continuity Plan
- BMS - Business Management System
- BOY – Beginning of (Fiscal) Year

EHE PWS

- BPM – Business Process Monitor (key piece of performance monitoring software)
- C&A – Certification and Accreditation
- CA – Certification Agent
- CAC – Common Access Card
- CARS – Cyber Asset Reduction and Security
- CCB – Configuration Control Board
- CCR – Central Contractor Registration
- CCM – Configuration & Change Management
- CCMP – Configuration & Change Management Plans
- CDA - Central Design Agency
- CEC – Civil Engineering Corps
- CI - Configuration Item
- CIAM – Command Information Assurance manager
- CIO – Command Information Officer
- CLIN – Contract Line Item Number
- CM - Configuration Management
- CMMI - Capability Maturity Model Integration
- CMP – Configuration Management Board
- CNO – Chief of Navy Operations
- COB – Close Of Business
- COE – Common Operating Environment
- CONUS - Continental United States
- COOP – Continuity of Operations Plan
- COR – Contracting Officer's Representative
- CoS - Continuity of Service
- COTS – Commercial-off-the-shelf
- CPI - Continuous Process Improvement
- CPU – Central Processing Unit
- CTR – Contract Technical Representative (NMCI term)
- CVS – Contractor Verification System
- CYE – Calendar Year End
- DAA – Designated Approval Authority
- DADMS – Department of the Navy Applications and Database Management System
- DBMS – Data Base Management System
- DCPDS – Defense Civilian Personal Data System
- DECC – Defense Enterprise Computing Center
- DEERS – Defense Enrollment Eligibility Reporting System
- DFAR – Defense Federal Acquisition Regulation
- DIACAP – DoD Information Assurance Certification and Accreditation Process
- DISA – Defense Information Systems Agency
- DITSCAP – DoD Information Technology Security Certification and Accreditation Process
- DMS – Defense Messaging System
- DoD – Department of Defense
- DODD – Department of Defense Directive
- DODI – Department of Defense Instruction
- DON – Department Of Navy
- DR - Disaster Recovery
- DSS – Decision Support System
- DWAS – Defense Working capital fund Accounting System
- EI – Enterprise Integration
- E2E - End to End
- EOY – End Of (Fiscal) Year
- EP – Execution Plan
- ESRI - Environmental Systems Research Institute (a leading geographic information systems vendor)

FHS PWS

- EUL - End User Layer
- FAM – Functional Area Manager
- FAR – Federal Acquisition Regulation
- FAQ – Frequently Asked Questions
- FEC – Facilities Engineering Command
- FISMA - Federal Information Security Management Act
- FMO - Financial Management Office
- FTE - Full-Time Equivalent
- FY – Fiscal Year
- GF – General Fund
- GIS – Geographic Information Systems
- GPO – Group Policy Objects
- GPS – Global Positioning System
- HVAC – Heating, Ventilation and Air Conditioning
- HTMLDB – Hyper Text Markup Language Data Base (an Oracle Portal Development Environment)
- IA – Information Assurance
- IAM – Information Assurance Manager
- IAO – Information Assurance Officer
- IAT – Information Assurance Technical
- IAVA – Information Assurance Vulnerability Alert
- IAVB – Information Assurance Vulnerability Bulletin
- IAW – In Accordance With
- IAWF - Information Assurance Work Force
- IMMEDIATE - No more than 30 minutes
- INFOCON - Information Operations Condition
- INFOSEC - Information Security
- IPT – Integrated Product Team
- IT – Information Technology
- ITIL - Information Technology Infrastructure Library
- IV&V – Independent Verification and Validation
- J2EE – Java Version 2 Enterprise Edition
- JPAS – Joint Personal Adjudication System
- JSP - Java Server Pages
- LDAP – Lightweight Directory Access Protocol
- LNS – Legacy Network Shutdown
- LUN – Logical Unit
- HPQC - HP Quality Center (Formerly Mercury Quality Center)
- NACLA – National Agency Check with Local Agency
- NAS – Network Attached Storage
- NASP - NAVFAC Application Service Provider
- NAVFAC – Naval Facilities Engineering Command
- NBVC – Navy Base Venture County
- NET – Navy Enterprise Transportation
- NGEN - Next Generation (Navy-owned network)
- NAVNETWARCOM – Navy Network Warfare Command
- NFELC – Naval Facilities Expeditionary Logistics Center
- NITC – NAVFAC Information Technology Center
- NMCI – Navy Marine Corps Intranet
- NTR – Navy Technical Representative
- NWCF – Navy Working Capital Fund
- OAPEX - Oracle Application Express
- OAS - Oracle Application Server
- OCONUS – Outside Continental United States
- OCB - Operations Control Board
- OCS – Oracle Collaboration Suite

FHEB PWS

- ODAA – Operations Designated Approval Authority
- OEM – Oracle Enterprise Manager
- OFM - Oracle Fusion MiddleWare
- OID – Oracle Internet Directory
- OLTP - On Line Transactional Processing
- ONE-NET – OCONUS Navy Enterprise Network
- OO – Ordering Officer
- OS – Operating System
- OST – Operational Support Team
- PBSOW – Performance Based Work Statement
- PEO-EIS – Program Executive Office for Enterprise Information Systems
- PKE – Public Key Enabling
- PKI – Public Key Infrastructure
- POA&M – Plan of Actions and Milestones
- POC – Point Of Contact
- PW – Public Works
- PWS – Performance Work Statement
- QA/CM – Quality Assurance/Configuration Management
- QASP – Quality Assurance Surveillance Plan
- QC – Quality Control
- QI Session - Quality Improvement Sessions (Process Validation/Audit)
- QTP – Quick Test Professional
- RDMBS – Relational Data Base Management System
- RFA – Request for Action
- RFC - Request for Change
- ROI – Return on Investment
- SA – System Administrator
- SAAR – System Authorization Access Request
- SAN – Storage Area Network
- SCADA – Supervisory Control and Data Acquisition
- SECNAV – Secretary of the Navy
- SDE – Spatial Data Engine
- SDP – System Decision Paper
- SLIN – Sub Line Item Number
- SPAWAR – Navy Space Warfare Command
- SPM – Single Platform MAXIMO®
- SRR - System Readiness Review
- SSBI – Single Source Background Investigation
- SSL – Secure Sockets Layer
- ST&E – Security Test & Evaluation
- STIG – Security Technical Implementation Guide
- TF – Task Force
- Tier 1 support – Response and routing of user initiated telephone help calls, emails and online submissions from the CIO Support Tracking System on the NAVFAC Portal.
- Tier 2 support – Advanced response to help calls referred from Tier 1.
- TOM – Task Order Manager
- TPS – Test Plan/Script
- TR - Technology Refresh
- TRM – Total Resource Management
- TS - Technology Stack
- TSO – Time Sharing Option
- UPS – Uninterrupted Power Supply
- USC – US Code
- VUGen – Virtual User Generator (Mercury product for creating monitoring plans and scripts)

FHS PWS

3. Enterprise Hosting Services (EHS) Contract Description And Deliverables

Introduction/Summary All tasks in this contract require IAT Level II "privileged access", Refer to paragraph 1.2.1, Clearances and Licensing for mandated requirements, and SECNAV M-5239.2 (Appendix G - OS Commercial Certification). Services and functions required include recurring sustainment requirements and surge requirements described below.

A. Hardware, Operating Systems, Utility Tools, and Internal Network Sustainment Support

These are recurring and routine day-to-day tasks that support the daily operations, maintenance and sustainment of all hosting infrastructure across all environments. Description of work are detailed in Section 3.1, and Section 3.4 thru Section 3.7. Skill level requirements range from entry-level to journeyman level unless otherwise specified.

General work requirements include:

1) Server builds, server/parts replacement, cloning, configuration. Includes SUN/Oracle, Dell and HP platforms in physical and virtual environments, rack placement, asset tagging and labeling.
2) Operating System and other administration software installation, configuration, and maintenance. Includes patches, release updates, component updates, system log reviews, archiving.
3) Citrix Infrastructure Management (XenApp Server, XenApp Client/Desktop) including software/tools installations, client access, printer setup, user profile management
4) System tuning, service availability monitoring, performance optimization
5) Network device management and administration. Includes Domain Name Servers, Lightweight Directory Access Protocol, Domain Controllers, Network Switches and panels, Cables,
6) Internal network management. Includes cabling, inter-connection, end to end cable labeling,
7) Enterprise Shared Storage management and allocations. Includes drive/parts replacements, usage monitoring, system alert monitoring and troubleshooting, redundancy configuration, capacity planning, and provisioning. Storage infrastructure include: Sun/Oracle, EMC, NetApp, DataDomain
8) Backup management and administration. Includes reviewing backup logs, re-running jobs, automating backup jobs, scheduling jobs, data replication to COOP/DR site
9) Vulnerability assessments, STIG and FISMA compliance. Including administration and management of available security tools (example: NESSUS, HBSS, RETINA, TRIPWIRE)
10) Service Request Fulfillment. This includes all service requests received via the Service Tracking System (STS), or emails and phone calls from senior management or from the NITC Operations Watch for any call-back off-hours service support.
11) Standardization, Continuous Process Improvement and Documentation. This includes writing scripts and shell codes for automating recurring tasks, developing/modifying system administration processes, change and configuration tracking

Skill sets required to fulfill this requirement include :

- Server Administrators (Solaris, Linux, Windows, Citrix)
- Storage Administrators
- Backup Administrators
- VMWare Administrators

At a minimum, the Contractor shall provide qualified and skilled resources for key positions identified in Attachment 04 to sustain the day-to-day operations of the hosting infrastructure.

Contract Deliverables:
C0001 - Fully qualified and skilled personnel for Key Positions #1 thru #4

EHS PWS

B. <u>Enterprise Database Sustainment Support</u>

These are recurring and routine day-to-day tasks that support the daily operations, maintenance and sustainment of all enterprise databases hosted across all environments. Database platforms currently hosted include: Oracle Enterprise RDBMS, MSSQL Server, SYBASE. Most database environments are configured on stand-alone server platforms. Mission critical databases are configured for redundancy using Oracle RAC, Oracle Dataguard, MSSQL Cluster. Description of work are detailed in Section 3.2, and Section 3.4 thru Section 3.7. Skill level requirements range from journeyman to senior level unless otherwise specified.

General work requirements include:

1) Installation, configuration, and maintenance of database software suite, and other database administration tools. This includes patches, release updates, one-off patches, component updates, client software, plug-ins.
2) Database/instance creation, configuration, management and administration. This includes datafiles, tablespaces, tables, schema, ddl & dml objects.
3) Resource usage monitoring, augmentation and cleanup. This includes storage, memory, CPU, network bandwidth and throughput,
4) Database system tuning, service availability monitoring, performance monitoring and optimization, SQL script analysis and tuning
5) Client server connectivity, system interface and integration, external & internal links
6) User access and privileges management
7) Backup and restoration using manual and automated methodologies. Includes reviewing backup logs (from RMAN, scripts, and other backup utilities), scheduling, recovery testing to ensure integrity of backup jobs, fixing and re-running jobs
8) Vulnerability assessments and FISMA compliance. Includes performing database SRR scans, mitigations, and resolutions; quarterly Oracle CPU patches; IAVs
9) Service Request Fulfillment received via Service Tracking System (STS), emails and phone calls from senior management or from the NITC Operations Watch for any call-back off-hours service support. This include promotion requests from various CDA developers.
10) Standardization, Continuous Process Improvement and Documentation. This includes writing scripts and shell codes for automating recurring tasks, developing/modifying database administration processes, change and configuration tracking

Skill sets required to fulfill this requirement include :

- Oracle Database Administrators
- MS SQL Server Database Administrators

At a minimum, the Contractor shall provide qualified and skilled resources for key positions identified in Attachment 04 to sustain the day-to-day operations of enterprise databases hosted at the NAVFAC Data Center.

<u>Contract Deliverable</u>:
C0002 - Fully qualified and skilled personnel for Key Positions #5 and #6

C. <u>Applications and Technology Stack Sustainment Support</u>

These are recurring and routine day-to-day tasks that support the daily operations, maintenance, and sustainment of all technology stacks supporting all business systems hosted across all environments. Core technology stacks include: Oracle; Microsoft; SAP; ESRI; HP; Adobe; IBM;

EHS PWS

F5. Specific software products are listed in Attachment 03 - Technology Stacks and Hosting Services. Applications technology stack infrastructure configuration varies from stand-alone to a multi-server multi-tier redundant and scalable configuration. Deployment techniques are either Web-based or CITRIX-based. Description of work are detailed in Section 3.3 thru Section 3.7. Skill level requirements range from entry-level to journeyman level unless otherwise specified.

General work requirements include.

1) Installation, configuration, and maintenance of application software suites listed above and their supporting components, tools and plugins. This include patches, release updates, one-off patches, component updates, client software & add-ons.
2) Configuring and maintaining redundant and high-available application configuration
3) Configuring and monitoring system interfaces, integration, user connectivity
4) Configuring secure application delivery using encryption methodologies which include: secure socket layer (SSL) or Transport Layer Security (TLS) for all business systems (includes: HTTPS, SFTP)
5) Integration between common access card (CAC) and public key infrastructure (PKI)/single sign-on (SSO) for secure application access
6) Managing user access, accounts and system privileges
7) Managing application and web services, monitoring service availability
8) Application performance tuning and optimization
9) Resource usage monitoring, augmentation and cleanup. This includes storage, memory, CPU, network bandwidth and throughput
10) Client server connectivity, system interface and integration, user access and privileges management
11) Vulnerability assessments including IAV patching, quarterly CPU updates, SRR/STIG fixes and mitigations, IA POA&M actions. This includes security implementations for web servers and application servers
12) Service Request Fulfillment received via Service Tracking System (STS), emails and phone calls from senior management or from the NITC Operations Watch for any call-back off-hours service support. This include code promotion requests from various CDA developers.
13) Standardization, Continuous Process Improvement and Documentation. This includes writing scripts and shell codes for automating recurring tasks, developing/modifying system and application administration processes, change and configuration tracking

Skill sets required to fulfill this requirement include :

- Maximo System Administrators
- Oracle Application Administrators
- GIS Application Administrators
- Citrix-based Application Administrators
- COGNOS Systems Administrators
- HP Software Systems Administrators
- IIS Web Site Administrators
- MS Sharepoint Administrators

At a minimum, the Contractor shall provide qualified and skilled resources for key positions identified in Attachment 04 to sustain the day-to-day operations of the technology stacks infrastructure and all business systems hosted therein.

Contract Deliverable:
C0003 - Fully qualified and skilled personnel for Key Positions #7 and #8

FHG PWS

D. <u>Emerging Systems and Large Projects Support</u>

Surge requirements for large hosting projects requiring more than 120 billable hours of effort. See Section 2.6 for the definition of "large hosting projects". The NAVFAC Data Center estimates approximately two to three large projects per year requiring additional personnel with specialized skill-sets in functional areas A, B and C above. Work requirements are described in Section 3.7. Skill level requirements range from senior level to master level unless otherwise specified.

General work requirements include:

- Technical consulting, researching, analyzing, project planning, system architecture and design, infrastructure topology, network engineering, and presentation of recommendation to management
- Hands-on technical implementation (includes installation, configuration, integration, migration from legacy systems, and systems deployment)
- System documentation, transitioning to in-house support (includes: training in-house support)

Skill sets required to fulfill this requirement vary from each project.

<u>Contract Deliverable</u>:
C0004 - Fully functional and documented system
C0005 - Fully trained in-house support

EHS PWS

3.1. Hosting Infrastructure Operations, Sustainment, and Maintenance Support

3.1.1 Server Administration

Background: The NITC server infrastructure currently include approximately 200+ physical servers and 300+ Operating systems.

The NAVFAC Data Center is implementing it's IT Roadmap initiative to comply with Navy's effort of server footprint reduction, Green IT, consolidation and virtualization. The goal is to reduce the number of physical servers up to 45% within a three-year period from the start of this contract, but still be able to provide IT services required to host and support all business systems listed in Attachement 01 without impact to availability and performance.

Server Administration Services include: Backup and Restoration Services, Host Base Security System, Domain/User Administration, Vulnerability Assessment, Shared Storage Services, Mail Relay Services, Secure File Transfer Services, Secure Server Access Services, Secure Application Delivery Service, Citrix Infrastructure Management Service, Infrastructure Management Service, Port and Protocols Management Service, Software and Hardware Life Cycle Management Support.

3.1.1.a Server build and configuration

Overview: The contractor shall provide technical support in installing, building, and configuring all servers which include: HP, Dell and Sun/Oracle servers that comprise the NITC hosting environments (ie: DevCOI and EDMZ). This includes hardware support for ongoing installation, configuration and maintenance of all servers running Microsoft Windows, RedHat Linux, and SUN/Oracle Intel operating systems; development, implementation and maintenance of configuration standards and technical server administration procedures; and administration of network devices (ie: Domain Name Servers, Active Directory, LDAP, network devices, peripheral devices, switches, cables, port panels).

The contractor shall coordinate, discuss, and validate tasks requirements and system impacts, hardware and software resource availability, and prioritization with the Government Technical Lead or designated representative.

The Contractor shall attend meetings dealing with servers related issues (i.e., support, maintenance, changes and/or upgrades) and communicate those issues to the government technical lead or designated representative.

The contractor shall provide hardware services support to prepare for and conduct load testing. Load testing shall be conducted to identify impacts to system performance and to identify performance bottlenecks. All load testing activities shall be performed on the environment designated by the Government.

The contractor shall provide hardware services support for the COOP/DR site.

Work Description: The contractor shall be responsible for the installation, configuration, and sustainment of all servers which include: HP, Dell, and Sun/Oracle servers running Microsoft Windows, Redhat Linux and Sun/Oracle operating systems. This will include but not be limited to the daily, weekly and monthly sustainment and maintenance of each hardware device. Tasks shall be performed in accordance with established NITC change management procedures. This includes the following tasks:

EHSPWS

- Working with DBA and Application Administration staff to determine optimal hardware system configuration.
- Updating servers with newer hardware components and parts.
- Participating in the testing of system software and hardware components.
- Configuring servers for load balancing, redundancy, and fail over.
- Configuring servers for standalone or virtual environment as required.
- Capacity monitoring and management

Objectives:

A. Provide server builds and configuration for the hosting environments
B. Provide server builds and configuration for the COOP/DR site
C. Comply with standard hardware configuration
D. Troubleshoot hardware problems.
E. Provide server availability, optimization, and tuning.
F. Comply with servers life cycle management
G. Coordinate server changes to the COE

Performance Deliverables:

P0001 - Standard Dell Server Standalone Configuration Checklist
P0002 - Standard Dell Server Virtual Configuration Checklist
P0003 - Standard HP Server Standalone Configuration Checklist
P0004 - Standard HP Server Virtual Configuration Checklist
P0005 - Standard Sun/Oracle Server Standalone Configuration Checklist
P0006 - Standard Sun/Oracle Server Virtual Configuration Checklist

3.1.1.b Software Installations, Updates and Configuration

Overview: The contractor shall provide technical support in installing and configuring all operating systems and other server administration tools that support the NITC hosting environments (ie: DevCOI, EDMZ and COOP/DR). This includes technical support for ongoing installation of software release updates and version upgrades, configuration, and maintenance patches of all server administration tools and operating systems (ie: MS Windows Enterprise/Standard, RedHat Linux/Redhat, and Sun/Oracle Solaris); development, implementation and maintenance of configuration standards and administration procedures; and administration of network protocols and services that support applications hosted in each server.

The contractor shall coordinate, discuss, and validate tasks requirements and system impacts, software license availability, and prioritization with the Government Technical Lead or designated representative.

The Contractor shall attend meetings as needed dealing with OS related issues (i.e., support, maintenance, changes and/or upgrades) and communicate those issues to the government technical lead or designated representative.

The contractor shall provide OS services support to prepare for and conduct load testing. Load testing shall be conducted to identify impacts to system performance and to identify performance bottlenecks. All load testing activities shall be performed on the environment designated by the Government.

The contractor shall provide operating system services support for the COOP/DR site.

EITS PWS

Work Description: The contractor shall be responsible for the installation and operation of all Operating System (OS) and server administration tools in the NITC hosting environments. This will include but not be limited to the daily, weekly and monthly sustainment and maintenance of each operating systems. Tasks shall be performed in accordance with established NITC change management procedures. This includes the following tasks:

- Research, analyze impact, install, and test software updates, patches and hot fixes.
- Manage and maintain user and group accounts and Group Policy Objects (GPO).
- Provide support for user and file management (ie: local accounts, file sharing, drive mappings, file permissions, security profiles)
- Ensuring compatibility of utility and applications software with the OS.
- Ensure connectivity and interoperability between systems.
- Understand and comply with STIG (Security Technical Implementation Guidelines), SRR (System Readiness Review), and Information Assurance Vulnerability Alert/Bulletin (IAVA/B) guidance that applies to the operating system platforms in the hosting environment.
- Work with DBA and Application Administration staff to troubleshoot and resolve operational problems.
- Participate in the testing of system software components.
- Schedule newly configured system for backup to include operating systems and file systems
- Develop and test scripts to automate recurring system administration functions and provide supporting documentation.

Objectives:

A. Provide software installation and configuration for the hosting environments
B. Provide software installation and configuration for the COOP/DR site
C. Comply with standard operating systems configuration
D. Troubleshoot operating system problems.
E. Provide operating systems optimization, and tuning.
F. Comply with software life cycle management
G. Coordinate operating system changes to the COE

Performance Deliverables

P0007 - Standard Windows OS Standalone Configuration Checklist
P0008 - Standard Windows OS Virtual Configuration Checklist
P0009 - Standard Linux/RedHat OS Standalone Configuration Checklist
P0010 - Standard Linux/RedHat OS Virtual Configuration Checklist
P0011 - Standard Solaris OS Standalone Configuration Checklist
P0012 - Standard Solaris OS Virtual Configuration Checklist

EHS PWS

3.1.2 Enterprise Storage Administration

Background: NITC owns and maintains four Netapp v3160 controllers and one Netapp FAS v3140 controller with over 800 Terabytes of raw storage capacity of both SAS and SATA drives. The Netapp devices support production data with the v3160 controllers supporting primary site storage and the FAS v3140 supporting COOP storage. NITC also has three Sun 6540 storage systems that support pre-production storage. NITC supports NAS, SAN and CIFS/NFS storage allocations.

3.1.2.a Enterprise Storage Configuration

Overview: The contractor shall be responsible for basic management of the enterprise shared storage systems. The contractor shall ensure all shared storage systems are operating as expected, replication between primary and COOP controllers is operating and that interfaces to backup storage are configured properly

The contractor shall coordinate, discuss, and validate requirements and prioritization with the Government Technical Lead or designated representative.

The contractor shall provide hardware services support for the COOP/DR site.

The Contractor shall attend meetings dealing with storage related issues (i.e., support, maintenance, changes and/or upgrades) and communicate those issues to the government technical lead or designated representative.

Work Description: The contractor shall be knowledgeable in configuring redundant storage systems for high availability and data integrity. This includes the following tasks:

- Configure, maintain, and monitor data replication between NITC hosting facility and the COOP/DR site
- Configure, maintain, and monitor interconnectivity between the storage device and client servers
- Monitor system alerts, troubleshoot and resolve problems
- Work with government technical lead or vendors for parts replacements to resolve hardware problems
- Develop and maintain storage configuration item checklist
- Coordinate storage configuration changes to COE
- Track changes to the systems
- Develop, execute and maintain roll-back procedure to ensure the system can be restored to its previous working state.
- Develop and maintain storage architecture diagram showing drive capacity, connections, RAID configuration.
- Comply with hardware life cycle management
- Comply with NITC Change Management and Configuration Management procedure
- Perform capacity planning and management

Objectives:

A. Ensure that all storage systems are configured to support replication to COOP/DR site
B. Ensure that all storage systems are configured to support backup operations.
C. Ensure that all storage systems are configured to support various types of storage allocations (NAS, SAN, CIFS/NFS)
D. Ensure that all systems can be restored back to its previous working state during failed maintenance.

Performance Deliverables:

EHS PWS

P0013 - SAN Storage configuration checklist
P0014 - NAS Storage configuration checklist
P0015 - CIFS/NFS Storage configuration checklist
P0016 - SAN Device architecture diagram

3.1.2.b Storage Allocation

Overview: The contractor shall be responsible for allocating, and deallocating storage as required. The contractor shall have working knowledge of properly allocating storage and a good understanding of NITC's COOP requirements and storage limitations.

The contractor shall coordinate, discuss, and validate requirements and prioritization with the Government Technical Lead or designated representative prior to allocating/deallocating storage.

Work Description: The contractor shall be responsible for executing storage allocation requests. Tasks include:

- Allocating new storage, deallocating existing storage, and modifying capacity of existing storage allocation.
- Complying with change and configuration management policies to ensure storage requests are approved.
- For new or additional storage requests, the contractor shall confirm with government technical lead or designated representative prior to executing the request. The contractor shall perform analysis of new storage requests and provide configuration recommendation.
- Continuously track and report storage useage
- The contractor shall track allocations/deallocations and coordinate such changes to COE.
- Provide storage alloction services for COOP/DR site

Objectives:

A. Ensure production storage is allocated properly to maintain replication process with COOP site.
B. Monitor storage useage and allocation of the COOP/DR site.
C. Ensure storage types are properly configured.
D. Report on storage utilization and growth trends
E. Comply with NITC change and configuration management policies.

Performance Deliverables:

P0017 - Storage Utilization and Growth Trends Report

EHS PWS

3.1.3 Backup Administration

Background: NITC uses several backup systems as part of its integrated backup strategy. These systems include: Oracle/Sun x4540 (Thumper) servers, EMC Data Domain DD880 virtual tape library, Oracle/Sun Sparc and StorageTeck SL500 tape backup devices. NITC runs EMC Networker Enterprise Backup software on all servers to run backup jobs. All of these systems are used as part of NITC's backup strategy. The process is designed to pass data between systems as the data is passed through the backup process.

3.1.3.a Backup Device Configuration

Overview: The contractor shall be responsible for installation, managing and configuring the backup system.

Work Description: The contractor shall ensure that all backup devices are configured according to NITC specifications. Tasks include:

- The contractor shall be able to add additional devices in order to expand the capacity of each system. This may include adding a tape drive to the SL500 library or adding a disk shelf to the DD880.
- The contractor shall ensure the devices continue to operate as required after failed components are replaced.
- Comply with change and configuration management policies to changes to backup systems are approved.
- The contractor shall track all changes and coordinate such changes to COE

Objectives:

A. Ensure all backup devices are working properly
B. Configure to reduce data duplication
C. Configure to compress data as much as possible.

Performance Deliverables:

P0018 – Standard Backup Device Configuration Checklist

3.1.3.b Backup jobs management

Overview: The contractor shall configure, manage and administer all backup jobs using the EMC networker to execute server system backups. The contractor shall be knowledgeable with capacity-based license model that allows it to run backup jobs against all servers and pays for the amount of data that is backed-up.

Work Description : The contractor's tasks include:

- Scheduling backup jobs on all servers and storage devices.
- Monitoring backup jobs to ensure they complete successfully.
- Resolve backup job errors and failures as they occur.
- Create tape backups and package for off-site storage

Objectives:

A. Ensure all operating systems, file systems, application data are backed-up
B. Mimize impact of backup jobs.

Performance Deliverables:

P0019 – Daily report identifying the status of previous night's backup
P0020 – Daily report identifying the progress of resolving backup job failures.
P0021 – Monthly report confirming that all servers have backup jobs scheduled.

EHS PWS

3.1.4 Networking and inter-connectivity

Background: NITC administrators manage the internal network and inter-connectivity while working closely with the Navy's network provider, NMCI/NGEN, in enabling end-user access to the systems. Attachment 02 describes the NITC hosting regions which include DevCOI (Experimental, Development, Test) and eDMZ (Acceptance, Production, COOP/DR).

Overview: The contractor is responsible for configuring and managing NITC's internal network and inter-connectivity while working closely with the Navy's network provider, NMCI, to allow end-users access to systems hosted at NITC. The NITC hosting regions include DevCOI (Experimental, Development, Test) and eDMZ (Acceptance, Production, COOP/DR). In addition, NITC maintains a backend network to allow management and communication between servers and storage devices. NITC Networking devices include Brocade, Foundry, and Juniper.

NITC owns and maintains 19 Brocade SAN fiber channel switches, 26 Foundry gigabit network switches, 2 Infiniband switches and 2 Juniper 10gE switches that support all storage and backup data transfer requirements for NITC.

The contractor shall attend meetings as required dealing with networking and interconnectivity issues, and communicate to government technical leads or designated representatives.

The contractor shall provide remote support for administering the internal network supporting the COOP/DR site

Work Description: The contractor shall be responsible for the installation, maintenance and operation of the network infrastructure devices in the NITC hosting environments. This will include but not be limited to the daily, weekly and monthly sustainment and maintenance of each network device. Maintenance will be performed in accordance with established NITC change management procedures. This includes the following tasks:

- Manage and maintain the configuration of all network devices.
- Ensuring compatibility between 1gE and 10gE connections..
- Research, analyze impact, install and test patches and hot fixes.
- Ensure connectivity and interoperability between servers and clients.
- Comply with STIG (Security Technical Implementation Guidelines), SRR (System Readiness Review), and Information Assurance Vulnerability Alert/Bulletin (IAVA/B) guidance that applies to the network system platforms in the hosting environment.
- Add, modify or remove physical connections between network devices and servers.
- Participate in the testing of network hardware components.
- Comply with NITC change management policies and procedures

Objectives:

A. Provide server inter-connectivity and system integration
B. Provide technical support in troubleshooting NMCI network issues
C. Maintain all NITC owned network devices and ensure accessibility to all servers
D. Develop and maintain tracking inventory of all network devices, IPs, ports, and protocols

Performance Deliverables:

P0022 - Network Tracking Inventory

EHS PWS

3.1.5 Optimization and Performance Tuning

Overview: Optimization is an ongoing task required for successful hosting operation.

Work Description: The Contractor shall perform optimization and tuning in all areas of the hosting infrastructure (ie: servers, operating systems, storage and backup). Tasks include monitoring performance, analysis of results, recommendation for optimization/tuning, implementation, performance validation, and documentation of changes.

The contractor shall gather and provide system utilization statistics for management reporting; monitor systems for resource-intensive activity and take corrective action when necessary; perform capacity planning and system benchmarking; monitor space, CPU and memory usage on servers; and analyze, optimize and tune the system for optimum performance.

The contractor shall provide technical support to prepare for and conduct load testing. Load testing shall be conducted to identify impacts to system performance and to identify performance bottlenecks. All load testing activities shall be performed on the environment designated by the Government.

Objectives:

A. Provide recommendations for optimization and performance tuning.

EHS PWS

3.1.6 Software and Hardware Maintenance Support

Overview: NITC is responsible for taking all steps necessary to ensure the health and optimal operation of all servers, operating systems, backup and storage devices. Software and Hardware Maintenance Support refers to recurring tasks that are not explicitly assigned but that are required in order for the continuous operation of the hosting infrastructure. These tasks are normally performed during non-core hours and weekends.

Work Description: The contractor shall identify all recurring maintenance tasks necessary to maintain the operation of the servers, operating systems, backup and storage devices. Maintenance tasks include those tasks identified by the government as mandatory, and items identified by the contractor as necessary to maintain the operation of the hosting environments. Tasks include but are not limited to:

- Archive log files
- Defragmenting storage space
- Locking/deleting obsolete accounts
- Update anti-virus signatures
- Update configuration baselines
- Run system integrity diagnostics
- Apply patches, hot fixes, and updates
- Scan for unauthorized files/accounts/passwords
- Execute security scans and fix vulnerabilities
- Install/repair/replace hardware devices and peripheral devices
- Update maintenance spreadsheet
- Test all maintenance tasks and ensure successful completion of all tasks

For maintenance tasks not completed on schedule, the Contractor shall provide document stating reasons for delay.

The contractor shall comply with NITC change and configuration management procedures.

Objectives:

A. Identify and successfully complete all maintenance tasks as scheduled
B. Test all maintenance tasks prior to implementation in production
C. Develop roll-back procedure for major maintenance tasks to ensure service recovery
D. Coordinate maintenance tasks to impacted system stakeholders

Deliverables:

P0023 - Maintenance tasks list and status

EHS EWS

3.1.7 Hardware Refresh

Background: Periodic hardware refreshes occur in order to ensure all systems are fully supported by the vendor, and to ensure systems do not reach obsolescence that will impact systems availability.

Overview: The contractor shall support ongoing server refreshes to ensure up-to-date and valid vendor support. The contractor shall identify hardware resources that are needing replacements and provide installation and configuration supports necessary to bring devices on-line.

Work Description: The contractor shall develop detail work schedule and technical steps needed to:

- Migrate legacy systems to new systems
- Analyze, test, configure systems in either stand-alone or virtual environment
- Analyze, test, configure systems interfaces and interconnectivity
- Install operating systems and related components
- Transfer applications and data to the new hardware

The contractor shall continuously identify hardware resources that are nearing end-of-warranty or end-of-service/life, and notify government technical lead or designated representative for appropriate replacement acquisition action.

The contractor shall have knowledge of and familiarity with NITC's virtualization technology, and systems high-availability and redundancy requirements.

The contractor shall be able to identify networking and hardware components that can provide efficient deployment of refreshed servers.

The contractor shall implement and maintain a high-available and redundant architecture while performing technology refreshes.

The contractor shall comply with established NITC change management policies, and NITC Life Cycle Management procedures.

Objectives:

A. Ensure all servers, network and storage devices have current maintenance and warranty contracts to prevent obsolescence or end-of-service (EOS) or end-of-life (EOL).
B. Develop strategy for implementing new server or storage replacements without major impact to services and applications hosted at the NITC
C. Perform risk analysis and compatibility issues prior to full implementation
D. Minimize outages during the refresh.

Performance Deliverables:

P0024 - Hardware refresh implementation schedule
P0025 - Fully supported hardware

EHS PWS

3.2. Enterprise Database Operations, Sustainment, and Maintenance

3.2.1. Database Systems Administration

Background: The NITC Data Center currently hosts approximately 260+ Oracle databases, 16+ Sql Server databases, and 10+ Sybase databases. Types of databases supported include:

- OLTP (Online transaction processing system), traditionally used for real-time transaction system used to carry out day to day business functions
- OLAP (Online Analytical Processing), used for providing analysis and running huge queries efficiently without impacting real-time processing
- Geographic information system databases (ESRI's ARCSDE) which captures, stores, analyzes, manages, and presents data with reference to geographic location data
- Reporting databases which pulls data from various systems for reporting
- Datawarehouse & Datamart

Databases and instances are hosted on heterogenous server platform (ie: Sun Sparc Solaris, Windows 2003 and Windows 2008), using enterprise storage devices (ie: NetApp, Sun SAN, EMC), and configured from simple stand-alone servers to a redundant and high-available architecture using Oracle RAC, Oracle DataGuard, MSSQL Server Clusters, or the F5 Big IP load balancer features.

NITC DBA staff administration tools for managing the databases include: Oracle Enterprise Manager, MS SQL Server Management Studio, Sybase Central and Interactive SQL.

3.2.1.a Database Software Installation and Configuration.

Overview: The contractor shall have a working knowledge of Solaris, Linux, and Windows operating systems in which the databases are hosted, the underlying database technologies, redundant architecture, and the business systems being supported. The contractor shall be knowledgeable of RAID configuration techniques.

The contractor shall confirm schedule with the NASP Technical Lead who is responsible for acquiring management approval to proceed.

Work Description: The contractor shall be responsible and accountable for properly installing and configuring database software upgrades, release updates, component upgrades, one-off patches; and installing, managing and administering database management tools authorized for use in the NITC hosting facility. Tasks include:

- The Contractor shall ensure all NITC change management and portfolio management requirements are met and complied with.
- Coordinating with NASP technical leads and CDA representatives in developing detail work breakdown schedule (WBS) and POA&M
- Ensuring all necessary software, licenses, hardware, and storage resources are available and ready for use. This includes defining required directory structures, permissions, RAID configuration, ports, protocols, interfaces
- Installing, configuring, and testing RDBMS software component updates and new software releases
- Installing, configuring, testing, and using database management software and tools (ie: Oracle Enterprise Manager, MS SQL Server Management Studio, Sybase Central and Interactive SQL, TOAD, SQL Plus)
- Developing software installation and update/upgrade procedure

EHS PWS

- Developing roll-back procedure to ensure upgrades/updates are restored back to its previous working state.
- Developing and maintaining standard database binaries configuration item checklist
- Understand, configure, maintain, and document network interfaces between systems
- Executing SRR scan immediately after software install to baseline its security posture
- Scheduling system backup immediately after software is installed and configured

Objectives:

A. Execute POA&M and WBS on schedule
B. Maintain security posture of all database installations
C. Ensure all database binaries and datafiles are backed-up
D. Comply with software life cycle management
E. Comply with portfolio and change management procedures
F. Coordinate changes to COE

Performance Deliverables:

P0026 - Work Breakdown Schedule (WBS)
P0027 - Database Binaries Standard Configuration Checklist
P0028 - Software Installation Procedure
P0029 - Network Interfaces document

3.2.1.b Database and Instance Creation and Configuration

Overview: The contractor shall have a working knowledge of Solaris, Linux, and Windows operating systems in which the databases are hosted, the underlying database technologies, redundant architecture, and the business systems being supported. The contractor shall be knowledgeable of RAID configuration techniques. This task shall be performed after approval by the NITC Operations Control Board (OCB).

Work Description: The contractor is responsible for identifying server and storage resources; and coordinating change to government technical lead.

Prior to creating databases or instances in a co-hosted environment, the contractor shall perform risk analysis to ensure existing systems are not impacted.

The contractor is accountable for creating and configuring databases and instances based on NASP configuration standards, and customer requirements. The contractor shall ensure databases and instances are built and configured for optimum availability and performance. The contractor shall ensure database/instance configuration consistency across environments.

The contractor shall configure, test and maintain database inter-connectivity and inter-operability between systems and clients. This includes creating new or modifying existing TNSNames, TNS Listeners, DNS entry, host name entry, CIFS/NFS, shares, ODBC, ODP .Net, or direct connections.

The contractor shall ensure databases and instances created meet the database STIG and SRR requirements prior to releasing to customers. Initial security scans shall be used for baselining its security compliance.

EHS PWS

The contractor shall ensure that all newly created databases and instances are immediately scheduled for backup prior to releasing for use. The contractor shall account for all databases (new and existing) in the backup scheduling tools.

The contractor shall develop, execute and maintain Standard Operating Procedures and related documentations which include:

- Standard database and instance creation procedure
- Standard database and instance configuration checklist
- Database backup and restore procedure
- Automation scripts for creating basic databases/instances
- Database and systems interfaces list
- System dependency hierarchy diagram

The contractor shall maintain an inventory of all databases hosted at NITC. This includes but not limited to: configuration items list, server name, TNS-name, listener, ODBC dataset name, business systems it supports, assigned DBA, schemas, storage, power users, privileges. Inventory shall be readily available to the government when needed.

The contractor shall comply with NITC change management and configuration management procedures.

Objectives:

A. Create and configure databases using high-availability architecture
B. Automate database and instance creation
C. Develop new or update existing database standard operating procedures
D. Develop security compliance baseline for newly created database or instance
E. Schedule newly created databases and instances for backup before releasing to customers
F. Incorporate newly created databases and instances in established service monitoring tools

Performance Deliverables:

P0030 - SOP for creating databases and instances
P0031 - Database and instance standard configuration checklist
P0032 - Database backup and restore procedure
P0033 - Automation scripts for creating basic databases and instances
P0034 - Database and systems interfaces list
P0035 - System dependency hierarchy diagram

3.2.1.c Database Monitoring, Optimization and Tuning

Overview: Database optimization is an ongoing task required for successful hosting operation. The contractor shall be very familiar with, and experienced in using the performance analysis tools available at the NASP. Contractor shall research availability of other performance monitoring solutions and make recommendations for possible implementation at the NASP.

Work Description: The Contractor shall perform monitoring performance, analysis of results, recommendation for optimization/tuning, implementation, performance validation, and documentation of changes.

The contractor shall perform day-to-day performance monitoring and optimization tasks which include:

EHS PWS

- Gather and provide database utilization statistics and trends for management reporting;
- Monitor, maintain and configure system for optimal performance in conjunction with application and database requirements;
- Monitor systems for resource-intensive activity and take corrective action when necessary;
- Perform capacity planning and system benchmarking;
- Monitor storare, CPU and memory usage on servers;
- Analyze, optimize and tune databases for optimum performance.

The contractor shall provide technical support to prepare for and conduct load testing specially on major data migration. Load testing shall be conducted to identify impacts to system performance and to identify performance bottlenecks. All load testing activities shall be performed on the environment designated by the Government.

The contractor shall perform quality control analysis of all sql scripts provided by the CDA prior to execution. The contractor shall recommend modifications to fine tune the sql script for better performance.

The contractor shall comply with the NASP standard procedure for database monitoring, and ensure all tasks specified therein are completed successfully and performed at specified intervals or frequency. The contractor shall use Oracle Enterprise Manager, Unix Cron Schedule, HP Business Service Monitor and other available tools for monitoring jobs

The contractor shall monitor specific database functions and processes to determine if thresholds are exceeded. When thresholds are exceeded, the contractor shall take corrective action as specified in the NASP standard procedure for database monitoring.

Objective:

A. Implement recommendations for optimization and performance tuning.
B. Comply with NASP standard procedure for database monitoring
C. Gather performance statistics and develop trend reports
D. Perform load testing on major data migration prior to production deployment

Performance Deliverables:

P0036 - Performance statistics and trend reports

EHS PWS

3.2.1.d Database Backup and Restoration.

Overview: The NITC Data Center ensures that all databases can meet recovery point objectives and recovery time objectives as specified in each applications' service level agreement (SLA). For applications without a formal SLA, NITC shall provide a recovery point objective of no more than 24 hours from the time of failure, and a recovery time objective of no more than 12 hours, depending on the size of the database. NITC has a formal plan for backing up all databases that describes the methods and tools available to perform backups.

Work Description: The contractor shall execute backups as necessary to ensure the ability to comply with recovery objectives as defined in the SLA. The contractor shall perform periodic database recoveries to ensure backups are working as expected. The contractor shall have some expertise of using RMAN to perform database backups and of Netapp snapshot software for database backups. Backup and recovery tasks include:

- Schedule backup jobs for every database as required to meet SLA.
- Monitor jobs and correct any erros or failures.
- Report major issues that may jeopardize ability to meet SLA.

New databases shall have backup jobs scheduled before they are released to the requestor. The contractor shall monitor all backup jobs and troubleshoot all job errors and failures as necessary to be able to meet the SLA. If contractor cannot resolve backup errors, the contractor shall immediately notify government with a comprehensive analysis of the issue.

Objectives:

A. Ensure all databases have appropriate backup jobs scheduled
B. Ensure all database backups can meet SLA requirements
C. Validate backups with test restores

Performance Deliverables:

P0037 – Backup schedule log
P0038 – Automated job status report
P0039 – Database test restore plan

3.2.1.e Database Sustainment and Maintenance.

Overview: The contractor shall perform daily sustainment support to all databases hosted at NITC. Maintenance tasks shall be performed during non-core hours and weekends. Sustainment and maintenance tasks are to be performed in compliance with NITC change and configuration management procedure.

Work Description: The contractor shall perform maintenance tasks during specified maintenance windows and as necessary to ensure the environment remains stable. Tasks include:

- Manage and perform promotions of packages, codes and data.
- Research, analyze, install and test software patches, updates and hot fixes.
- Develop and implement maintenance checklist and roll-back procedure
- Provide maintenance tasks in the "Weekend Maintenance Schedule"
- Perform batch data migrations
- Database structure modifications (ie: create tables, tablespace, index, triggers, procedures)

The contractor shall ensure all maintenance tasks are fully tested in pre-production environments prior to implementation. Maintenance task status shall be reported in accordance with NITC change and configuration management procedures.

The contractor shall provide operational sustainment tasks which include managing user and system accounts, passwords, and privileges.

The contractor shall review all system logs and perform regular file system clean-up for optimum storage useage.

Performance Objectives:

A. Successfully complete all scheduled maintenance tasks
B. Maintenance tasks not completed as scheduled are justified

EHS PWS

3.3 Applications Technology Stack Operations, Sustainment, and Maintenance

3.3.1 COTS/GOTS Systems Administration

Background: The NAVFAC Data Center currently hosts a myriad of enterprise business systems (Attachment 01) across the hosting environments. In addition, NITC also offers IT services that supports all NAVFAC sites, all Navy Regions, the Marine Corps, and select private business partners. NITC's core technology stacks and hosting services are listed in Attachment 03. Attachment 02 - Common Operating Environment provides a picture of existing applications technology stacks and their infrastructure makeup.

3.3.1.a COTS/GOTS Software Component Updates and Configuration

Overview: The NAVFAC Data Center currently hosts all business systems listed in Attachment 01 in a heterogeneous hardware platforms (Sun Sparc, HP, Windows), operating systems (Solaris, Linux, Windows 2003/2008) connecting to enterprise SAN/NAS storage devices. While some application services are hosted in single-server stand-alone environments, most of the critical business systems are hosted within multi-tier, multi-server, and redundant configuration for high availability.

The contractor shall confirm schedule with the NASP Technical Lead who is responsible for acquiring management approval to proceed.

Work Description: The contractor shall be responsible and accountable for properly installing and configuring software updates, component upgrades, and one-off patches. Tasks include:

- Compliance with NITC change management and configuration management requirements
- Timely completion of tasks as defined by the NASP Technical Lead and approved by the NITC OCB.
- Develop checklist of all required resources and interfaces which include: software licenses, servers, storage, directory structures, system/service account, permissions, ports, protocols, interfaces, systems impact.
- Document installation, update, upgrade steps and configuration parameters.
- Develop roll-back procedure to ensure applications are restored back to their previous working state during failed upgrades, updates, patches, or service packs installations.
- Understand, configure, maintain, and document network interfaces between systems
- Coordinating with NASP Server Administrators to perform SRR scans immediately after applying software patch and component updates installation.
- Apply security fixes and mitigate any security findings resulting from security scans (includes: SRR scans, IAV, manual checklists).
- Review vulnerability scans, SRRs, and checklists and fix/mitigate security findings.
- Coordinating with NASP Backup Administrator to perform system backups immediately after applying software patches and component updates

EHS PWS

- Ensuring all software patches and component update installations are fully tested in the DevCOI environment prior to implementation in EDMZ (Acceptance and Production) hosting environment.

Objectives:

A. Execute tasks correctly and on schedule
B. Maintain security posture of all systems
C. Ensure all application binaries and codes are backed-up
D. Develop roll-back procedures for software updates and/or code promotions
E. Comply with change management and configuration management procedures
F. Coordinate changes to COE

Performance Deliverables:

P0040 - Installation Steps and Configuration Parameter List
P0041 - Roll-back Steps

EHS PWS

3.3.2 Business Systems and Web Sites Administration

3.3.2.a Systems Integration, Interface, connectivity, User Access

Overview: The contractor shall gain familiarity with the business processes employed by business systems listed in Attachment 01. The contractor shall be very familiar with NITC technology stacks and hosting services offered at NITC and identified in Attachment 03. While some business systems are hosted in their stand-alone environments, most are co-hosted in the same technology stacks within their own work space allocations. Shared technology stack infrastructure are configured so as to prevent processing over-flows thus corrupting other business systems performance and integrity.

Work Description: The contractor shall maintain business systems interfaces to ensure full functionality and accessibility. Tasks include:

- Ensure all application services are operational and functional in DevCOI (Experimental, Development, test) and EDMZ (Acceptance and Production)
- Provide technological support to developers for testing application interfaces
- Configure systems interconnectivity, internal and external interfaces, and system dependencies.
- Document system dependencies and interfaces
- Manage user access and privileges
- Comply with NITC change and configuration management processes

The contractor shall document all configuration items applied in each environment, and track all changes as they are implemented. This information shall be stored in a central repository that can be readily queried by the government as needed.

The contractor shall be responsible for configuring integration between internal and external systems interfaces and services to ensure full functionality and user accessibility. External interfaces and services can include: Big IP, Single-Sign-On, LDAP authentication, Mail Relay, Secure File Transfer, Database Services, Licensing Services, Performance Monitoring Services, Citrix Services, Domain Name Services, Report Generation Services, Share Storage, Backup and Restore Services.

The contractor shall ensure all changes to the environment are fully tested in the DevCOI prior to implementing in Acceptance and Production regions. This include all COTS and GOTS configuration changes and codes promotions.

The Contractor shall comply with NITC change and configuration management policies and procedures.

Objectives:

A. Ensure all application services are operational and available
B. Maintain application configuration item inventory
C. Configure all internal and external systems interfaces
D. Comply with change management procedures

Performance Deliverables:

P0042 - Business Systems Interfaces document
P0043 - Updated Configuration Items Checklist

EHS PWS

3.3.2.b Applications Sustainment and Maintenance

Overview: NITC is responsible for taking all steps necessary to ensure the health and optimal operation of all applications and hosting services. Applications and hosting services maintenance support refers to recurring tasks that are not explicitly assigned but that are required in order for the continuous operation of the applications technology stacks. These tasks are normally performed during non-core hours and weekends.

Work Description: The contractor shall identify all recurring maintenance tasks necessary to maintain the various technology stacks. Maintenance tasks include those tasks identified by the government as mandatory, and items identified by the contractor as necessary to maintain the operation of the hosting environments. Tasks include but are not limited to:

- Software component release patches
- One-off patches
- Security mitigations and patches
- Application log cleanups and archival
- Update configuration items
- Recycling application services
- Clear up run-away processes and service accounts
- Test maintenance tasks and ensure successful completion of all tasks
- Application code promotions

For maintenance tasks not completed on schedule, the Contractor shall provide document stating reasons for delay.

The contractor shall comply with NITC ITIL processes.

Objectives:

A. Identify and successfully complete all maintenance tasks as scheduled
B. Test all maintenance tasks prior to implementation in production
C. Comply with NITC ITIL processes
D. Coordinate maintenance tasks to impacted system stakeholders

Performance Deliverables:

P0044 - Maintenance tasks list and status

EHS PWS

3.3.3 Performance Monitoring, Optimization and Tuning

Overview: Performance monitoring, optimization and tuning is an ongoing task required for successful hosting operation. The contractor shall be very familiar with, and experienced in using the performance analysis tools available at the NASP.

Work Description: The Contractor shall monitor service availability and performance, analyze availability and performance reports, recommend for optimization/tuning, implementation, performance validation, and documentation of changes.

The contractor shall perform day-to-day performance monitoring and optimization tasks which include:

- Review application availability statistics and develop trends reports for management;
- Configure system for optimal performance in coordination with CDA, DBAs, Server and Storage administrators
- Monitor systems for resource-intensive activity and take corrective action when necessary;
- Analyze, optimize and tune hosting services for optimum performance.

The contractor shall provide technical support to prepare for and conduct load testing specially on major application promotions. Load testing shall be conducted to identify impacts to system performance and to identify performance bottlenecks. All load testing activities shall be performed on the environment designated by the Government.

The contractor shall ensure all application codes provided by the CDA for promotion into the Acceptance and Production regions are reviewed and successfully tested to ensure performance is not impacted. Errors detected shall be documented and codes returned to CDAs for rework, and contractor shall be able to roll-back changes if performance is severely degraded.

Objective:

A. Implement recommendations for optimization and performance tuning.
B. Gather performance statistics and develop trend reports
C. Perform load testing on major data migration prior to production deployment

Performance Deliverables:

P0045 - Performance and Availability Trend Reports

EHS PWS

3.4 Incident Response, Service Request Fulfillment and Tracking

3.4.1 Service Request Fulfillment

Overview: NITC adopted the ITIL framework to manage incident and service request tickets. Consistent with the ITIL framework, NITC's Operations Watch provide advanced service desk functions to create and track all incidents and service requests using online service and issue tracking systems. The contractor can reference ITIL documentation to determine the nature and type of work that will be assigned in service request tickets.

Work Description: The contractor shall ensure all incident and service request tickets are immediately acknowledged, and work started and completed according to NITC policy and as indicated in the incident or service request ticket. Contractor shall gain familiarity and understanding of the NITC internal policies on handling incident and service request tickets and issue escalation procedures.

The Contractor shall provide Tier 2 and Tier 3 support for any issues pertaining to hardware, operating systems, storage, backup systems, database systems, and applications services. Tier 2 and Tier 3 support notices may be received by telephone, email request or via an online support tracking system. Support may be rendered by telephone, email or collaboration tools.

The Contractor shall log all responses and actions taken in the online support tracking system. Contractor shall develop exception report for responses exceeding response time threshold.

Objectives:

A. Compliance with NITC's incident and service request policies
B. Compliance with NITC's issues escalation procedure
C. Successfully restore service.
D. Timely acknowledgement and response to incident and service requests.
E. Log all requests for assistance in appropriate tool.

Performance Deliverables:

P0046 – Incident Action Reports
P0047 – Exception report

3.4.2 Incident Response and Call-Back Support

Overview: The NITC Data Center supports NAVFAC operations worldwide 24 hours per day, 365 days per year. While direct support is provided during core hours, 0600 – 1800 M-F, NITC provides diagnostic and troubleshooting support 24 hours per day. In order to comply with NITC escalation procedures, the contractor shall be properly equipped to provide support within 15 minutes of receiving a call for assistance from the NITC OpsWatch.

Work Description: The contractor shall provide support for unplanned after-hours call-backs to troubleshoot and correct system problems. The Government estimates that this requirement of fulfilling call-backs and system maintenance responsibilities will total approximately 10% of server, operating system, storage, backup, database, and application system administration workload.

EHS PWS

The contractor shall be available to provide call-back support on a 24/7/365 basis. The contractor shall provide call-back support to resolve any issues that impact the availability of systems hosted at NITC. Issues that cause production downtime or causes work stoppage are categorized as urgent.

The contractor shall have the necessary equipment to respond within the specified timeframe. If necessary, contractor shall be prepared to report on-site at NITC to troubleshoot and resolve call-back issues.

The contractor shall provide diagnostic and troubleshooting services for any systems that become unavailable. All call-back work shall be reported on an Incident Report which include brief description of issue, impact to systems, root cause, and actions taken to resolve the issue. Should the issue be outside NITC's responsibility, the contractor shall follow escalation procedure.

Objectives:

A. Troubleshoot production call-backs 15 minutes upon receipt of notification.
B. Resolve issues successfully
C. Document all call-back actions
D. Comply with NITC Issues Escalation Procedure

Performance Deliverables:

P0048 - Call-Back Incident report
P0049 - Contractor on-call list

EHS PWS

3.5 Security Scans, Fixes, Mitigation Actions and Tracking

Overview: The NITC Data Center ensures that the hosting facility and all business systems hosted therein are fully accredited, have authority to operate (ATO), and are compliant with the Federal Information Security Management Act (FISMA). Security guidance, policies and requirements are provided by DOD, NAVY, DISA, NAVFAC IA Team and the local NITC IA team.

NITC employs automated tools to implement IT security requirements. These tools currently include: RETINA, HBSS, NESSUS, TRIPWIRE, SRR. Additional manual checklists are performed as prescribed by higher authorities.

Although the Contractor is responsible for daily security sustainment of all systems in the hosting center, FISMA review and re-accreditation process is performed annually and as needed as functionality changes are implemented for the business systems listed in Attachment 01. This requires ensuring that all systems are regularly scanned, and if vulnerabilities are detected, that they are fixed and/or mitigated.

Work Description: The Contractor shall maintain the security posture of the NITC hosting environments. The contractor shall be very familiar with the STIG requirements and guidelines outlined in FISMA with regards to operating system, data-at-rest, hardware, networks, application and web services, databases, user accounts and privileges. Using government prescribed security scanning tools, the contractor shall be responsible for performing security scans, implementing security patches and fixes, and developing mitigation actions. This will include but not be limited to the daily, weekly and monthly implementation of required security fixes. Information systems security implementations will be performed in accordance with established NITC change management procedures. This includes the following tasks:

- Performing security scans, checks, patches, and fixes.
- Understand and comply with STIG (Security Technical Implementation Guidelines), SRR (System Readiness Review), and Information Assurance Vulnerability Alert/Bulletin (IAVA/B).
- Research and analyze IAV patches and vendor specific patches as soon as published by software/hardware vendors
- Install and test security patches, and advice government technical lead or designated representatives of any impact to hosting services
- Develop checklist and roll-back plan for implementing patches and fixes
- Assist in CAC/PKI enabling initiatives for accessing systems in the hosting center
- Comply with NITC Change Management policies and procedures

Objectives:

A. Comply with IA, FISMA, and INFOCON requirements to achieve full ATO
B. Perform up-to-date security scans and submit scan reports to a designated central repository
C. Perform up-to-date security fixes and mitigation actions to ensure FISMA compliance
D. Provide clean Retina scans
E. Maintain security compliance at the COOP/DR site
F. Develop and implement IA tracking mechanisms

Performance Deliverables

P0050 - Security scans, manual security checklists and mitigation action reports

EHS PWS

3.6 Standardization, Continuous Process Improvement, and Documentation

Overview: Throughout the life of this Contract, the contractor shall maintain all standard operating procedures to ensure continuity of service.

Work Description: The contractor shall develop, execute and maintain standard operating procedures for maintaining the enterprise hosting environment.

Objectives:

A. Develop, execute and maintain NASP standard operating procedures for administering the NITC hosting environments
B. Comply with NASP documentation template
C. Comply with Continuous Process Improvement

EHS PWS

3.7 Emerging Systems, Large Projects, and Emerging Technology Support

Background: These are surge requirements for large hosting projects requiring more than 120 billable hours to accomplish. This includes: major infrastructure/hardware refreshes requiring data or application migration; major software version upgrades; establishing new hosting service platforms; emerging technologies and delivery techniques; new software deployments, new business system hosting support. The 120 billable hours shall not include wait-time for the completion of the following: NMCI DM process for bringing servers on-line; IA accreditation process; Acquisition process; and software/application rationalization process. Government estimates two to three large projects per year.

3.7.1 System Requirements Review

Overview: The Contractor shall work with the NASP Government Technical Lead or designated representative to understand business and organizational requirements.

The Contractor shall develop a comprehensive analysis document that include all hardware, OS and storage requirements. The Government will review and approve the completed requirements analysis document, ensuring that the document is approved by all stakeholders and project sponsors before work proceeds.

Objectives:

A. Perform research and analysis of customer requirements

Performance Deliverables:

P0051 - System Requirements Analysis Document

3.7.2 Technological Analysis and Design

Overview: The contractor shall provide technological analysis support using the System Requirements Analysis Document as a source for technological analysis and design.

Work Description: The contractor shall document results of analysis in a systems analysis and design document, and shall develop a project management plan addressing: hardware and storage capacity, software features, system interfaces (external and internal), migration paths, risks, cost, level of effort, implementation strategies, system configurations, staffing, and work breakdown structure (WBS).

The contractor shall coordinate with the NASP Project Manager who provides technical guidance and oversight. The Contractor shall interface with the NASP Application Administrators, NASP Database Administrators, NASP Server and Storage Administrators, CDA representatives, and the IA staff to effectively perform the work required in this section.

Objectives:

A. Design system architecture including networking and systems interfaces.
B. Develop Project Management Plan.
C. Coordinate infrastructure and interface changes for COE updates

Performance Deliverable:

P0052 - System Technology Infrastructure Analysis Design Document

EHIS PWS

3.7.3 Execution and Status Tracking and Reporting

Overview: The Contractor shall use the System Technology Infrastructure Analysis Design Document, Project Management Plan, and Implementation Strategy as source documents to satisfy specified requirements. The Contractor shall interface with the NASP Technical Leads, NAVFAC CDA, and NITC IA staff to effectively perform the work required in this section. Tasks should take into account interfaces between systems, connectivity between client systems, user accessibility, impact to existing systems, security, standards and performance.

Work Description: The Contractor shall be responsible for updating statuses, analyses, recommendations, actions taken, and resolutions within the appropriate change management system. Requirement, schedule, and level of effort for each large scale project will be determined at time of request.

Contractor shall ensure that design and implementation comply with security policies and guidance.

The Contractor shall document all system interfaces, dependencies, configuration parameters and adhere to existing change and configuration management policy.

The Contractor shall work with in-house technical support for implementation of systems interfaces, access policies, security standards, and other process issues.

The Contractor shall coordinate meetings with project stakeholders for analysis and implementation of changes and ensure change requests are entered into appropriate change management systems.

The Contractor shall provide timely status reports to government. Issues discovered at execution shall be immediately reported to the government. Adjustment to the schedule and strategy shall be justified and remediated.

The Contractor shall implement and successfully test all tasks in the DEVCOI environment prior to implementing in the EDMZ.

Objectives:

A. Execute the Project Management Plan on schedule.
B. Coordinate changes to COE.
C. Timely status reporting

Performance Deliverables:

P0053 – Weekly Status Reports

3.7.4 Deployment, Training and Closeout

Overview: Provide support for the deployment of new business systems and emerging technologies. This phase of the surge requirement means that the hosting infrastructure is ready to be enabled on-line for service hosting, user access, or business system integration in a production mode. This work is usually performed during a maintenance weekend.

Work Description: The Contractor shall be responsible for deploying large projects per the Project Management Plan. The Project Management Plan shall be coordinated with the appropriate NASP Technical Lead for acquiring necessary OCB approvals.

EHS PWS

The Contractor shall provide hands-on training to NASP in-house support on maintaining the system. Installation and deployment documents shall be developed and turned over to the government 30 days prior to the production deployment period.

The Contractor shall be responsible and accountable for the initial deployment of the system, troubleshoot and resolve issues.

The Contractor shall ensure that systems perform at acceptable level determined by system stakeholders prior to close-out of project.

Objectives:
A. Provide fully functional hosting service
B. Proper knowledge transfer to in-house support
C. Document system configuration items, interfaces, dependencies

Performance Deliverables:
P0054 - System configuration items, interfaces and dependencies

3.8 Contract Management

Overview: Throughout the life of this contract, the contractor shall provide contract management support to ensure the successful and timely completion of all contract deliverables.

Work Description: The contractor shall be responsible for ensuring all contract deliverables are completed within the agreed upon schedule. Tasks include:

- Develop monthly coverage report for core hours and call-back hours
- Develop bi-weekly budget and burn rate reports
- Initiate and facilitate monthly contract reviews with government
- Attend management meetings as required

Objectives:
A. Provide contractor personnel coverage report
B. Provide contract status reports

Performance Deliverables:
P0055 - Monthly coverage report
P0056 - Bi-Weekly Budget and Burn Rate Report
P0057 - Monthly Contract Review Presentation

EHS PWS

3.9 Performance Requirements Summary Matrix

Item	Performance Objective	Performance Standard and Acceptable Quality Level (AQL)	Methods of Performance Assessment
3.1.1.a Server build and configuration			
3.1.1.a.A	Provide server builds and configuration for the hosting environments	Contractor shall demonstrate a mature server build process that ensures all servers are built according to specifications. All server builds shall be completed within 5 business days of requestand as specified • No more than 2% rework • Servers comply with STIG requirements as specified in SOP • Security controls are implemented • Configuration baseline is updated	Government will review objective for the following: A documented process exists for building and configuring servers. All requests for server builds and configuration are performed according to requirements.
3.1.1.a.B	Provide server builds and configuration for the COOP/DR site	Contractor shall demonstrate a mature server build process that ensures all servers are built according to specifications. All server builds shall be completed within 5 business days of requestand as specified • No more than 2% rework • Servers comply with STIG requirements as specified in SOP • Security controls are implemented Configuration baseline is updated	Government will review objective for the following: A document and process exists for building and configuring servers. All requests for server builds and configuration are performed according to requirements.
3.1.1.a.C	Comply with standard hardware configuration	Contractor shall maintain an accurate and comprehensive configuration baseline of each server • Configuration baseline shall be 98% accurate • 100% of all configuration changes are approved by change management board before they are made.	Specific configuration of each server is maintained and accurate

EHS PWS

3.1.1.a.D	Troubleshoot hardware problems.	All issues are escalated according to NITC incident response process. All unresolved issues are submitted to problem management process. A post resolution report is submitted to NITC within 3 business days of issue that details the issue and resolution. Any configuration changes are documented and made according to configuration and change management policies Contractor responds to troubleshooting request within 2 hours. Contractor creates troubleshooting checklist for each type of system. Contractor shall present checklist withing 15 business days after award of contract. Checklist shall contain basic steps every administrator is to perform when troubleshooting issue.	Government will review objective for the following: A general checklist exists for each type of system that describes basic troubleshooting tasks. All problems are escalated according to NITC incident response process. A post resolution report is submitted to government
3.1.1.a.E	Provide server availability, optimization, and tuning.	Contractor shall review baseline metrics for server availability and performance on a daily basis. • Contractor shall monitor performance and availability agains established baseline and provide detailed report whenever performance and availability fall below established baseline. Report shall be delivered within 2 business days of incident. • Contractor shall begin work on restoring performance and availability to baseline immediately after identifying issue. Contractor shall provide optimization and tuning support as requested • Contractor shall make recommendations to improve performance and/or availability based on empirical data. • Contractor shall provide expected performance and/or availability gains as a result of changes.	Government will review objective for the following: Government will review performance and availability reports to determine if they are within established baselines. Government shall review report on deviations from baselines to determine if they accurately identify the cause of deviation. Contractor shall review recommendations to determine if they are based on empirical data. If changes are implemented, Government shall review empirical data to determine if expected performance and/or availability gains were achieved.

EHS PWS

3.1.1.a.F	Comply with servers life cycle management	Contractor shall be prepared to execute technology refresh of hardware • Contractor shall develop technical plans to migrate to new systems of similar architecture • Contractor shall pursue strategy that minimizes outage	Government will review objective for the following: Contractor was able to migrate to new hardware with minimal outage. Contractor accurately identified outage requirements.
3.1.1.a.G	Coordinate server changes to the COE	All server changes are performed according to change and configuration management policies All server changes are approved by change management board prior to executing change. A test and rollback plan is created prior to implementing changes. The COE is updated immediately after implementing changes.	Government Review
3.1.1.b Software Installations, Updates and Configuration			
3.1.1.b.A	Provide software installation and configuration for the hosting environments	Contractor shall demonstrate a mature server build process that ensures all servers are built according to specifications. All software builds shall be completed within 5 business days of requestand as specified • No more than 2% rework • Servers comply with STIG requirements • Security controls are implemented • Configuration baseline is updated • Backups are scheduled prior to delivery of software. • Maintenance jobs are scheduled prior to deliver of software. • All requested features are installed.	Government Review

EHS NWS

3.1.1.b.B	Provide software installation and configuration for the COOP/DR site	Contractor shall demonstrate a mature server build process that ensures all servers are built according to specifications. All software builds shall be completed within 5 business days of requestand as specified • No more than 2% rework • Servers comply with STIG requirements • Security controls are implemented • Configuration baseline is updated • Backups are scheduled prior to delivery of software. • Maintenance jobs are scheduled prior to deliver of software. • All requested features are installed.	Government Review
3.1.1.b.C	Comply with standard operating systems configuration	Contractor shall maintain an accurate and comprehensive configuration baseline of each server • Configuration baseline shall be 98% accurate • 100% of all configuration changes are approved by change management board before they are implemented.	Government Review

EHS PWS

3.1.1.b.D	Troubleshoot operating system problems.	All issues are escalated according to NITC incident response process. All unresolved issues are submitted to problem management process. A post resolution report is submitted to NITC within 3 business days of issue that details the issue and resolution. Any configuration changes are documented and made according to configuration and change management policies Contractor responds to troubleshooting request within 2 hours. Contractor creates troubleshooting checklist for each type of system. Contractor shall present checklist withing 15 business days after award of contract. Checklist shall contain basic steps every administrator is to perform when troubleshooting issue.	Government Review
3.1.1.b.E	Provide operating systems optimization, and tuning.	Contractor shall review baseline metrics for operating system (OS) availability and performance on a daily basis. • Contractor shall monitor performance and availability agains established baseline and provide detailed report whenever performance and availability fall below established baseline. Report shall be delivered within 2 business days of incident. • Contractor shall begin work on restoring performance and availability to baseline immediately after identifying issue. Contractor shall provide optimization and tuning support as requested • Contractor shall make recommendations to improve performance and/or availability based on empirical data. • Contractor shall provide expected performance and/or availability gains as a result of changes.	Government Review

EHS PWS

3.1.1.b.F	Comply with software life cycle management	Contractor shall be ready to upgrade software as required by government. • Contractor shall develop technical plan to upgrade software • Contractor shall document risks • Contractor shall prepare test and rollback plans • Contractor shall pursue upgrade path the minimizes system outage	Government Review
3.1.1.b.G	Coordinate operating system changes to the COE	All OS changes are performed according to change and configuration management policies All OS changes are approved by change management board prior to executing change. A test and rollback plan is created prior to implementing changes. The COE is updated immediately after implementing changes.	Government Review
3.1.2.a Enterprise Storage Configuration			
3.1.2.a.A	Ensure that all storage systems are configured to support replication to COOP/DR site	Contractor shall maintain the configuration of storage system as required to replicate data between primary Netapp storage and COOP Netapp storage • Contractor shall evaluate any required patches and changes to SAN system for impact to replication circuit. Contractor shall provde written analysis of possible impact of patches and changes, 2 business days before executing change. • Contractor shall identify and execute tasks required to maintain the replication circuit functioning • Contractor shall monitor replication between SAN systems to ensure data is synchronized between systems. Contractor shall immediately begin work on restoring replication whenever an issue is discovered.	Government Review

EHS PWS

3.1.2.a.B	Ensure that all storage systems are configured to support backup operations.	Contractor shall maintain the configuration of storage system as required to replicate data between primary Netapp storage and COOP Netapp storage • Contractor shall evaluate any required patches and changes to SAN system for impact to backup operations. Contractor shall provde written analysis of possible impact of patches and changes, 2 business days before executing change. • Contractor shall identify and execute tasks required to maintain backup operations • Contractor shall monitor backup operations and immediately begin work on restoring backups whenever issues are identified.	Government Review
3.1.2.a.C	Ensure that all storage systems are configured to support various types of storage allocations (NAS, SAN, CIFS/NFS)	Contractor shall maintain the configuration of storage system as required to provide NAS, SAN and CIFS/NFS type storage. • Contractor shall evaluate any required patches and changes to SAN system for impact to storage allocations. Contractor shall provde written analysis of possible impact of patches and changes, 2 business days before executing change. • Contractor shall identify and execute tasks required to maintain storage operations • Contractor shall monitor backup operations and immediately begin work on restoring storage system whenever issues are identified.	Government Review
3.1.2.a.D	Ensure that all systems can be restored back to its previous working state during failed maintenance	Contractor shall provide test and backout plans for all changes. • Contractor shall be able to execute rollback plans if maintenance is determined to have failed. • Contractor shall provide rollback plans prior to every change. • Contractor shall perform a test restore of 2 systems per month.	Government Review

EHS PWS

3.1.2.b Storage Allocation			
3.1.2.b.A	Ensure production storage is allocated properly to maintain replication process with COOP site.	Contractor shall ensure storage allocation changes to primary storage system are also made to COOP site • Contractor shall ensure new storage allocations are configured on the COOP and replication is working within 1 business day of allocating primary storage.	Government Review
3.1.2.b.B	Monitor storage useage and allocation of the COOP/DR site.	Contractor shall provide usage reports of COOP storage system • Contractor shall provide details about available storage space. Information shall include total storage available, max amount of allocatable storage. • Contractor shall provide details about available allocation units (LUNs, CIFs, etc) • Contractor shall provide growth trends for storage use.	Government Review
3.1.2.b.C	Ensure storage types are properly configured.	Contractor shall ensure every storage allocation is configured according to government specifications	Government Review
3.1.2.b.D	Report on storage utilization and growth trends	Contractor shall provide usage reports of COOP storage system • Contractor shall provide details about available storage space • Contractor shall provide details about available allocation units (LUNs, CIFs, etc) Contractor shall provide growth trends for storage use.	Governmen tReview
3.1.2.b.E	Comply with NITC change and configuration management policies.	Contractor shall ensure all changes are approved by change management board prior to implementation Contractor shall ensure all changes to the configuration of the storage system are recorded in the configuration management database within 1 business day of implementing change.	Government Review
3.1.3.a Backup Device Configuration			

EHS EWS

3.1.3.a.A	Ensure all backup devices are working properly	Contractor shall monitor the operation of backup devices and take action to correct errors • Contractor shall report whenever device failure impact the ability to perform backups within 1 business day of detecting errors • Contractor shall begin work on fixing errors immediately after identifying issues.	Government Review
3.1.3.a..B	Configure to reduce data duplication	Contractor shall monitor data deduplication of VTL system agains established baselines • Contractor shall provide deduplication metrics to include deduplication ratios • Contractor shall perform maintenance necessary to maintion deduplication ratios • Contractor shall evaluate system to improve deduplication ratio • Contractor shall identify and resolve issues that cause deduplication ratios to exceed established baselines.	Government Review
3.1.3.a.C	Configure to compress data as much as possible.	Contractor shall monitor data compresion of VTL system against established baselines • Contractor shall provide compression metrics and report whenever compression ratios exceed established baseline • Contractor shall perform maintenance necessary to maintion compression ratios • Contractor shall evaluate system to improve compression ratio Contractor shall identify and resolve issues that cause compression ratios to exceed established baselines.	Government Review
3.1.3.b Backup jobs management			
3.1.3.b.A	Ensure that all operating systems, file systems, application data are backed-up	Contractor shall monitor backup jobs and provide daily reports of job backup status • Contractor shall begin work on correcting backup job failures 1 business day after job failure • Contractor shall immediately escalate to government any jobs that cannot be fixed within 1 business day.	Government Review

EHS PWS

3.1.3.b.B	Mimize impact of backup jobs.	Contractor shall distribute backup jobs to minimize resource requirements. Contractor shall scheduled to minimize overlap.	Government Review
3.1.4 Networking and inter-connectivity			
3.1.4.A	Provide server inter-connectivity and system integration	Contractor shall monitor and maintain systems inter-connectivity. • Contractor shall troubleshoot and resolve issues • Contractor shall immediately escalate to government any isses that cannot be fixed within 1 business day.	Government Review
3.1.4.B	Provide technical support in troubleshooting NMCI network issues	When requested, Contractor shall provide technical support to NMCI in troubleshooting network issues.	Government Review
3.1.4.C	Maintain all NITC owned network devices and ensure accessibility to all servers	Contractor shall ensure accessibility to all network devices	Government Review
3.1.4.D	Develop and maintain tracking inventory of all network devices, IPs, ports, and protocols	Contractor shall maintain a comprehensive inventory of all network devices in the hosting environment.	Government Review
3.1.5 Optimization and Performance Tuning			
3.1.5.A	Provide recommendations for optimization and performance tuning.	Contractor shall establish a resource utilization baseline for all servers. • Baseline shall consist of general resource utilization (CPU, memory, IO) • Contractor shall monitor actual resource utilization with baseline and report to government when baselines are exceeded • Contractor shall make monthly recommendations to reduce resource utilization Contractor shall implement approved recommendations according to change and configuration management processes.	Government Review
3.1.6 Software and Hardware Maintenance Support			
3.1.6.A	Identify and successfully complete all maintenance tasks as scheduled	Contractor shall maintain list of daily, weekly and monthy maintenance tasks. • Contractor shall execute maintanence tasks using approved maintenance windows Contractor shall follow approved change and configuration management policies.	Government Review

EHS PWS

3.1.6.B	Test all maintenance tasks prior to implementation in production	Contractor shall ensure all changes are executed and tested in all pre-production environments. • Contractor shall follow approved maintenance windows.	Government Review
3.1.6.C	Develop roll-back procedure for major maintenance tasks to ensure service recovery	Contractor shall provide roll-back procedures for all tasks at least 2 days prior to executing maintenance tasks.	Government Review
3.1.6.D	Coordinate maintenance tasks to impacted system stakeholders	Contractor shall provide notice of maintenance actions one week prior to execution. • Contractor shall evaluate feedback from stakeholders and provide analysis on expected impact.	Government Review
3.1.7 Hardware Refresh			
3.1.7.A	Ensure all servers, network and storage devices have current maintenance and warranty contracts to prevent obsolescence or end-of-service (EOS) or end-of-life (EOL).	Contractor is responsible for monthly reporting of warranty and osolescense status of all hardware. • Report shall include warranty expiration dates and EOSL dates. • Report shall highlight renewals that are due within six months.	Government Review
3.1.7.B	Develop strategy for implementing new server or storage replacements without major impact to services and applications hosted at the NITC	Contractor shall utilize strategy to migrate servers that results in least amount of downtime for the users. • For migration to similar platforms, outages shall not exceed two hours regardless of the size of the system. For migration to different platforms, contractor shall provide outage estimate using path the minimizes outage.	Government Review
3.1.7.C	Perform risk analysis and compatibility issues prior to full implementation	Contractor shall confirm full compatibility between server and target location. • Contractor shall identify and execute all tasks required to ensure full compatibility • Expectation is restricted to vendor published requirements. • In the event unpublished compatibility is discovered, contractor shall follow incident response policy.	Government Review
3.1.7D	Minimize outages during the refresh.	Contractor shall chose execution alternative that results in smallest outage window.	Government Review
3.2.1.a Database Software Installation and Configuration.			

EHS PWS

3.2.1.a.A	Execute POA&M and WBS on schedule	Perform all tasks as scheduled in the POA&M. Delays in schedule shall be justified and communicated to the government 3 days prior to encurring delays.	Government Review
3.2.1.a.B	Maintain security posture of all database installations	Contractor shall ensure all database installations are secure and access is granted to approved users. • Contractor shall ensure access to database binaries is restricted to approved users. Contractor shall ensure only required binaries are installed	Government Review
3.2.1.a.C	Ensure all database binaries and datafiles are backed-up	Contractor shall review and understand NITC policy regarding backup and recovery requirements. • Contractor shall ensure appropriate backups are scheduled as required by SLA and/or backup SOP • Contractor shall provide weekly status of backup and recovery • Contractor shall commence work to resolve any errors with backups 1 business day after error occurs. • Contractor shall immediately notify government whenever issues with backups place ability to meet SLA at risk. • Contractor shall perform monthly test restores of at least 2 systems.	Government Review
3.2.1.a.D	Comply with software life cycle management	Contractor shall be aware of NITC requirements and policy for software lifecycle management. • Contractor shall be prepared to upgrade systems are required to meet IA compliance requirements and to maintain software vendor support. • Contractor shall provide technical execution plans for upgrading software. Plan shall follow NITC policy for allowable maintenance windows. • Contractor shall execute upgrade plans as approved.	Government Review

EHS PWS

3.2.1.a.E	Comply with portfolio and change management procedures	Contractor shall ensure all changes to software are approved and recorded. • Contractor shall submit change requests are required by change management policy. • Contractor shall provide portfolio status update of all changes to portfolio management team.	Government Review
3.2.1.a.F	Coordinate changes to COE	Contractor shall coordinate changes to government technical lead within one day after completion of change	Government Review
3.2.1.b Database and Instance Creation and Configuration			
3.2.1.b.A	Create and configure databases using high-availability architecture	Contractor shall demonstrate expertise in Oracle RAC and SQL Server Clusters • Contractor maintain current Oracle and SQL cluster configurations • Contractor shall configure new installations of RAC and SQL within 10 business days of request.	Government Review
3.2.1.b.B	Automate database and instance creation	Contractor shall create and maintain database template to be used for the creation of new databases and instances • Template shall be fully IA compliant • Temaplate shall contain all maintenance and DBA items. • Contractor shall use template to create new databases within 1 business day of requests.	Government Review
3.2.1.b.C	Develop new or update existing database standard operating procedures	Contractor shall maintain SOP library • Develop new SOPs within 15 business days of requests • Update existing SOPs within 5 business days of requests	Government Review
3.2.1.b.D	Develop security compliance baseline for newly created database or instance	Contractor shall establish security baseline for all new databases • Baseline shall be taken within 5 business days AFTER application schema is loaded and approved. • Contractor shall maintain list of all mitigated vulnerabilities • Contractor shall validate appoved baseline with actual database state on a monthly basis • Contractor shall resolve new vulnerabilities within 30 calendar days of identifying new vulnerabilities	Government Review

EHSPWS

3.2.1.b.E	Schedule newly created databases and instances for backup before releasing to customers	Contractor shall ensure that database backup jobs exist for all databases before they are delivered to requestor.	Government Review
3.2.1.b.F	Incorporate newly created databases and instances in established service monitoring tools	Contractor shall ensure that all maintenance jobs and tasks are scheduled against new databases before they are released to requestor.	Government Review
3.2.1.c Database Monitoring, Optimization and Tuning			
3.2.1.c.A	Implement recommendations for optimization and performance tuning.	Contractor shall establish a resource utilization baseline for all databases. • Baseline shall consist of general resource utilization (CPU, memory, IO) • Contractor shall monitor actual resource utilization with baseline and report to government when baselines are exceeded • Contractor shall make monthly recommendations to reduce resource utilization • Contractor shall implement approved recommendations according to change and configuration management processes.	Government Review
3.2.1.c.B	Comply with NASP standard procedure for database monitoring	Contractor shall follow SOP for database monitoring • Contractor shall monitor all items identified in the SOP and in the required invervals • Contractor shall configure monitoring tool to automatically report status • Contractor is not expected to create manual reports.	Government Review
3.2.1.c.C	Gather performance statistics and develop trend reports	Contractor shall establish a resource utilization baseline for all databases. • Baseline shall consist of general resource utilization (CPU, memory, IO) • Contractor shall monitor actual resource utilization with baseline and report to government when baselines are exceeded • Contractor shall make monthly recommendations to reduce resource utilization Contractor shall implement approved recommendations according to change and configuration management processes.	Government Review

EHS EWS

3.2.1.c.D	Perform load testing on major data migration prior to production deployment	Contractor shall develop plan to execute load tests on databases • Contractor shall create scripts to measure processing capacity of each database. • Contractor shall perform load tests before and after major migrations to confirm that performance baselines are maintained.	Government Review
3.2.1.d Database Backup and Restoration.			
3.2.1.d.A	Ensure all databases have appropriate backup jobs scheduled	Contractor shall ensure backup strategy allows for compliance with SLAs. • Contractor shall execute backup strategy is required by NITC SOP. • Contractor shall validate existing backup strategy can meet SLA. Validation shall provide quarterly report describing expected RTO and RPO	Government Review
3.2.1.d.B	Ensure all database backups can meet SLA requirements	Contractor shall recommend adjustement to backup strategy if empirical data reveals strategy is not sufficient to meet SLA.	Government Review
3.2.1.d.C	Validate backups with test restores	Contractor shall conduct two test restores per month to determine if backups are valid and can be recovered. • Contractor shall provide report on test result to include actual recovery time and recover point metrics.	Government Review
3.2.1.e Database Sustainment and Maintenance.			
3.2.1.e.A	Successfully complete all scheduled maintenance tasks	Contractor shall maintain list of daily, weekly and monthy maintenance database maintenance tasks. • Contractor shall execute maintanence tasks using approved maintenance windows • Contractor shall follow approved change and configuration management policies.	Government Review
3.2.1.e.B	Maintenance tasks not completed as scheduled are justified	For all uncompleted tasks, contractor shall provide report detailing why task could not be completed. • Contractor shall provide details on areas that were outside the contractor's control.	Government Review
3.3.1.a COTS/GOTS Software Component Updates and Configuration			

EHS RWS

3.3.1.a.A	Execute tasks correctly and on schedule	Execute tasks on schedule. Should delays be expected, Contractor shall notify the government immediately. Reasons for delay shall be provided to government within 3 days after discovery of issue.	Government Review
3.3.1.a.B	Maintain security posture of all systems	Application and web server STIGS, IA Checklists, SRRs, and IAVAs are met, all required patches are applied and mitigations are documented on schedule.	Government Review
3.3.1.a.C	Ensure all application binaries and codes are backed-up	Confirmation that all application binaries and codes are backed up.	Government Review
3.3.1.a.D	Develop roll-back procedures for software updates and/or code promotions	Roll-back procedures are document and maintained every maintenance period and attached to the maintenance spreadsheet .	Government Review
3.3.1.a.E	Comply with change management and configuration management procedures	Confirm DADMS/NITEP entries with government technical leads on software release/version updates prior to implementation.	Government Review
3.3.1.a.F	Coordinate changes to COE	Coordinate software release/version change to government within 1 day of completion.	Government Review
3.3.2.a Systems Integration, Interface, connectivity, User Access			
3.3.2.a.A	Ensure all services are operational and available	Application services available at 99% levels or higher as reported by Performance Monitoring tools. Service availability below 99% must be reviewed, documented, and fixed.	Government Review
3.3.2.a.B	Maintain application configuration item inventory	Update configuration item inventory one day after implementation of change.	Government Review
3.3.2.a.C	Configure all internal and external systems interfaces	Business systems interfaces successfully configure and implemented.	Government Review
3.3.2.a.D	Comply with change management procedures	All changes to the environments shall go through the OCB process.	Government Review
3.3.2.b Applications Sustainment and Maintenance			
3.3.2.b.A	Identify and successfully complete all maintenance tasks as scheduled	All maintenance tasks completed as scheduled. Contractor shall maintain list of daily, weekly and monthy maintenance tasks. • Contractor shall execute maintanence tasks using approved maintenance windows Contractor shall follow approved change and configuration management policies.	Government Review

EHSOWS

3.3.2.b.B	Test all maintenance tasks prior to implementation in production	All maintenance tasks are first tested in non-production environment. Contractor shall follow approved change and configuration management policies.	Government Review
3.3.2.b.C	Comply with NITC ITIL processes	Contractor shall ensure systems are rolled-back to their working state should a maintenance change caused degradation or system availability issues.	Government Review
3.3.2.b.D	Coordinate maintenance tasks to impacted system stakeholders	Contractor shall ensure systems changes are communicated to all system stakeholders.	Government Review
3.3.3 Performance Monitoring, Optimization and Tuning			
3.3.3.A	Implement recommendations for optimization and performance tuning.	Analyze business systems performance using the HP toolset. Determine areas of improvement and submit recommendations to government within 5 business days of agreed upon schedule. Benchmark performance before and after implementation. Submit results to government one day after completion.	Government Review
3.3.3.B	Gather performance statistics and develop trend reports	Continuously review business systems performance using statistics reports generated by the HP performance monitoring tool. Report anomalies to the government within 1 day of discovery.	Government Review
3.3.3.C	Perform load testing on major data migration prior to production deployment	Perform load testing and document results within two days of agreed upon schedule.	Government Review
3.4.1 Service Request Fulfillment			
3.4.1.A	Compliance with NITC's incident and service request policies	Contractor shall have understanding of ITIL principles in order to comply with NITC's incident and service request policies • Contractor shall take actions to restore service as soon as possible • Contractor shall ensure service request tickets are acknowledge and completed according to policy Service request tickets shall be completed with no more than 2% rework	Government Review

EHS PWS

3.4.1.B	Compliance with NITC's issues escalation procedure	During an incident, if service cannot be restored within 30 minutes of troubleshooting, contractor shall follow incident response policy to contact government personnel AND open service request ticket with appropriate vendor.	Government Review
3.4.1.C	Successfully restore service.	Service is restored to its original working state	Government Review
3.4.1.D	Timely acknowledgement and response to incident and service requests.	Contractor shall immediately respond to all incidents Contractor shall acknowledge service request tickets within 2 business hours and complete request by the date specified in the request.	Government Review
3.4.1.E	Log all requests for assistance in appropriate tool.	Contractor shall ensure that all service requests are logged in the appropriate ticketing system within 1 business day of request. Contractor shall log actions taken and result within 1 business day.	Government Review
3.4.2 Incident Response and Call-Back Support			
3.4.2.A	Troubleshoot production call-backs 15 minutes upon receipt of notification.	Contractor shall ensure they are equipped to receive notification of incident or service request 24/7/365. Contractor shall ensure they are equipped to directly access systems within 15 minutes of incident notification. Contractor shall access systems and begin direct troubleshooting within 15 minutes of notification	Government Review
3.4.2.B	Resolve issues successfully	Contractor shall maintain the expertise necessary to resolve all issues successfully. • Contractor shall ensure they are aware of all available resources for resolving issues. • Contractor shall submit post-issue report for all issues that cannot be resolved within 1 business day. For prolonged issues, contractor shall be expected to demonstrate that issue was out of contractors control.	Government Review
3.4.2.C	Document all call-back actions	Contractor shall ensure all call-back actions are documted and all changes are done in accordance with change and configuration management policies.	Government Review

EHS FWS

3.4.2.D	Comply with NITC Issues Escalation Procedure	Contractor shall review and understand NITC incident escalation procedures. • Contractor shall ensure all personnel understand requirements. • Upon request, contractor shall provide post-incident report that identifies actions taken and specifies compliance. Report shall be provided 3 business days after request.	Government Review
3.5. Security Scans, Fixes, Mitigation Actions and Tracking			
3.5.A	Comply with IA, FISMA, and INFOCON requirements to achieve full ATO	Contractor shall review all IA compliance regulations and provide execution plan to resolve open findings • Contractor shall review IA requirements and provide government with report that details state of environment relative to IA requirements • Report shall note which IA controls are out of compliance. • Contractor shall provide plan for correcting areas that are out of compliance. Plan shall include description of change, if outages are required and potential changes in functionality. • Contractor shall execute changes to resolve findings after they are approved by change management board.	Government Review
3.5.B	Perform up-to-date security scans and submit scan reports to a designated central repository	Contractor shall ensure central scan repository is updated and accurate • Contractor shall ensure recurring scans are executed as scheduled. Contractor shall load scan results to repository database for tracking.	Government Review
3.5.C	Perform up-to-date security fixes and mitigation actions to ensure FISMA compliance	Contractor shall perform scans as requested to support accreditation efforts. • Contractor shall execute individual scans as requested and report findings • Contractor shall coordinate resolving open findings as required. Contractor shall ensure scans and resolutions are completed by the due date specified in the request.	Government Review

FISMA

3.5.D	Provide clean Retina scans	Contractor shall ensure all high Retina findings are resolved during the first approved maintenance window after a finding is identified.	Government Review
3.5.E	Maintain security compliance of servers at the COOP/DR site	Contractor shall ensure all COOP/DR servers remain compliant.	Government Review
3.5.F	Develop and implement IA tracking mechanisms	Contractor shall create and maintain a repository for tracking the IA status of all systems. • System shall be capable of storing the results of all scans and checklists. • System shall be capable of retrieving IA information of one or more systems. System shall be available within 30 business days from award of contract.	Government Review
3.6 Standardization, Continuous Process Improvement, and Documentation			
3.6.A	Develop, execute and maintain NASP standard operating procedures for administering the NITC hosting environments	Contractor shall be knowledgeable of the location of existing SOPs and use them in the performance of their tasks. Contractor shall maintain documents as needed.	Government Review
3.6.B	Comply with NASP documentation template	Contractor shall develop new SOPs within his/her designated area using the NASP document template.	Government Review
3.6.C	Comply with Continuous Process Improvement	Contractor shall identify areas of improvement in the SOPs and communicate them to the government with recommendations.	Government Review
3.7.1- Systems Requirements Review			
3.7.1.A	Perform research and analysis of customer requirements	Documents submitted for review within 5 days of receipt of customer requirements with less than 2% rework.	Government Review.
3.7.2 - Technological Analysis and Design			
3.7.2.A	Design system architecture including networking and systems interfaces.	Completion of analysis within 3 days of agreed upon completion date.	Government Review.
3.7.2.B	Develop Project Management Plan	Completion of Project Management Plan within 5 days of agreed upon completion date	Government Review.
3.7.2.C	Coordinate infrastructure and interface changes for COE updates		
3.7.3 - Execution and Status Tracking and Reporting			
3.7.3.A	Execute the Project Management Plan on schedule	Contractor shall perform tasks on schedule. Inform government of any issues that can delay task immediately after discovery of issue.	Government Review.

HTS PWS

3.7.3.B	Coordinate changes to COE	Coordinate change within 1 day of completion.	Government Review.
3.7.3.C	Timely status reporting	Contractor shall provide written status report once every week. Issues that can cause delay in execution shall be reported to government as soon as issue is known.	Government Review.
3.7.4 - Deployment, Training and Closeout			
3.7.4.A	Provide fully functional hosting service	Contractor shall test systems in pre-production environment. Resolve issues prior to deployment in production.	Government Review.
3.7.4.B	Proper knowledge transfer to in-house support	Contractor shall develop systems guide and manuals for turn-over to in-house support 30 days prior to full system deployment.	Government Review.
3.7.4.C	Document system configuration items, interfaces, dependencies	Contractor shall document system configuration items, interfaces, and depencies 30 days prior to project completion.	Government Review.
3.8 Contract Management			
3.8.A	Provide contractor personnel coverage report	Contractor shall provide monthly coverage report to government for: • core hours (0600-1800 M-F) • off-hours call-back support, and • maintenance weekend coverage	Government review
3.8.B	Provide contract status reports	Contractor shall provide: • Bi-weekly budget and burn rate report for every task order issued against this contract • Monthly financial and staffing status report • Monthly contract review with government to discuss overall health of the contract	Government review

EHS PWS

3.10 Deliverables

Item	Deliverable	Format	Date Required
3	C0001 - Fully qualified and skilled personnel for Key Positions #1 thru #4		Upon contract award. See Section 7.8 for proposing substitutions.
3	C0002 - Fully qualified and skilled personnel for Key Positions #5 and #6		Upon contract award. See Section 7.8 for proposing substitutions.
3	C0003 - Fully qualified and skilled personnel for Key Positions #7 and #8		Upon contract award. See Section 7.8 for proposing substitutions.
3	C0004 - Fully functional and documented system		Upon completion of large hosting project
3	C0005 - Fully trained in-house support		30 days prior to completion of large hosting project
3.1.1.a	P0001 - Standard Dell Server Standalone Configuration Checklist	Word Document	As Required
3.1.1.a	P0002 - Standard Dell Server Virtual Configuration Checklist	Word Document	As Required
3.1.1.a	P0003 - Standard HP Server Standalone Configuration Checklist	Word Document	As Required
3.1.1.a	P0004 - Standard HP Server Virtual Configuration Checklist	Word Document	As Required
3.1.1.a	P0005 - Standard Sun/Oracle Server Standalone Configuration Checklist	Word Document	As Required
3.1.1.a	P0006 - Standard Sun/Oracle Server Virtual Configuration Checklist	Word Document	As Required
3.1.1.b	P0007 - Standard Windows OS Standalone Configuration Checklist	Word Document	As Required
3.1.1.b	P0008 - Standard Windows OS Virtual Configuration Checklist	Word Document	As Required
3.1.1.b	P0009 - Standard Linux/RedHat OS Standalone Configuration Checklist	Word Document	As Required
3.1.1.b	P0010 - Standard Linux/RedHat OS Virtual Configuration Checklist	Word Document	As Required
3.1.1.b	P0011 - Standard Solaris OS Standalone Configuration Checklist	Word Document	As Required
3.1.1.b	P0012 - Standard Solaris OS Virtual Configuration Checklist	Word Document	As Required
3.1.2.a	P0013 - SAN Storage configuration checklist	Word Document	As Required
3.1.2.a	P0014 - NAS Storage configuration checklist	Word Document	As Required
3.1.2.a	P0015 - CIFS/NFS Storage configuration checklist	Word Document	As Required
3.1.2.a	P0016 - SAN Device architecture diagram	Visio Diagram	As Required
3.1.2.b	P0017 - Storage Utilization and Growth Trends Report	Excel SpreadSheet	As Required
3.1.3.a	P0018 – Standard Backup Device Configuration Checklist	Word Document	As Required
3.1.3.b	P0019 – Daily report identifying the status of	Word Document	As Required

EHS PWS

	previous night's backup		
3.1.3.b	P0020 – Daily report identifying the progress of resolving backup job failures.	Word Document	As Required
3.1.3.b	P0021 – Monthly report confirming that all servers have backup jobs scheduled.	Excel SpreadSheet	As Required
3.1.4	P0022 - Network Tracking Inventory	Excel SpreadSheet	As Required
3.1.6	P0023 - Maintenance tasks list and status	Excel SpreadSheet	As Required
3.1.7	P0024 - Hardware refresh implementation schedule	Excel SpreadSheet	As Required
3.1.7	P0025 - Fully supported hardware		As Required
3.2.1.a	P0026 - Work Breakdown Schedule (WBS)	Excel SpreadSheet	As Required
3.2.1.a	P0027 - Database Binaries Standard Configuration Checklist	Word Document	As Required
3.2.1.a	P0028 - Software Installation Procedure	Word Document	As Required
3.2.1.a	P0029 - Network Interfaces document	Visio Diagram	As Required
3.2.1.b	P0030 - SOP for creating databases and instances	Word Document	As Required
3.2.1.b	P0031 - Database and instance standard configuration checklist	Word Document	As Required
3.2.1.b	P0032 - Database backup and restore procedure	Word Document	As Required
3.2.1.b	P0033 - Automation scripts for creating basic databases and instances		As Required
3.2.1.b	P0034 - Database and systems interfaces list	Excel SpreadSheet	As Required
3.2.1.b	P0035 - System dependency hierarchy diagram	Visio Diagram	As Required
3.2.1.c	P0036 - Performance statistics and trend reports	HP Trend Report	As Required
3.2.1.d	P0037 – Backup schedule log	Word Document	As Required
3.2.1.d	P0038 – Automated job status report	Word Document	As Required
3.2.1.d	P0039 – Database test restore plan	Word Document	As Required
3.3.1.a	P0040 - Installation Steps and Configuration Parameter List	Word Document	As Required
3.3.1.a	P0041 - Roll-back Steps	Word Document	As Required
3.3.2.a	P0042 - Business Systems Interfaces document	Word Document	As Required
3.3.2.a	P0043 - Updated Configuration Items Checklist	Word Document	As Required
3.3.2.b	P0044 - Maintenance tasks list and status	Excel SpreadSheet	As Required
3.3.3	P0045 - Performance and Availability Trend Reports	HP Trend Report	As Required
3.4.1	P0046 – Incident Action Reports	Word Document	As Required
3.4.1	P0047 – Exception report	Word Document	As Required
3.4.2	P0048 - Call-Back Incident report	Word Document	As Required
3.4.2	P0049 - Contractor on-call list	Word Document	As Required
3.5	P0050 - Retina Scans, SRR scans and mitigation action reports		As Required
3.7.1	P0051 - System Requirements Analysis Document	Word Document	As Required
3.7.2	P0052 - System Technology Infrastructure Analysis Design Document	Word Document	As Required
3.7.3	P0053 – Weekly Status Reports	Word Document	Weekly
3.7.4	P0054 - System configuration items, interfaces and dependencies	Visio Diagram	As Required
3.8	P0055 - Monthly coverage report	Word Document	Monthly
3.8	P0056 - Bi-Weekly Budget and Burn Rate Report	Excel SpreadSheet	Bi-Weekly
3.8	P0057 - Monthly Contract Review Presentation	PowerPoint	Monthly

FOUO PWS

4. Quality Planning, Control And Assurance

Quality Assurance Surveillance Plan (QASP):
The quality assurance surveillance plan (QASP) outlines the framework and methods that will be utilized to provide surveillance and review of the Contractor's fulfillment of contract acceptance criteria and other contract standards, including its quality control plan execution. The Government shall develop the QASP and evaluate Contractor performance based on this framework. The Government will evaluate the overall project performance on a regular basis to provide confidence that the project will satisfy the relevant quality standards. The system shall be applicable to all subcontractors and members of the contractor's team, if appropriate.

Quality Control Plan (QC):
T he Contractor shall monitor the specific project results to determine that they comply with relevant quality standards and identify ways to eliminate causes of unsatisfactory performance through utilization of its Quality Control (QC) plan based on Project Management Institute (PMI) best practices.

The Contractor shall address the quality control planning, execution and tracking to be utilized to assure compliance with task order performance standards. The Contractor shall provide its quality control program in its technical proposal.

The contractor shall develop, implement and maintain a quality assurance program. The system shall included inspection, validation, evaluation, corrective action and procedures necessary to effect quality control of all performance and products under the contract. The system shall allow inspection and evaluation by the government.

5. Government Furnished Information, Services, And Equipment

The Government will furnish NMCI workstations and network resources, workspace, furnishings, office supplies, document reproduction, fax and telephone services, video-conferencing and web-conferencing necessary to accomplish assigned work covered by this Contract when some or all of the support must be performed in Government spaces.

The Government will make available relevant standards, functional statements, technical manuals, computer systems guides, reference material, regulations, instructions, and operational procedures necessary to accomplish this Contract.

The Government will provide Government Common Access Cards (CAC).

The Government will provide hand held equipment to accomplish assigned work covered by this Contract.

The Government will provide the required number of software licenses necessary to accomplish this Contract when support effort is required to be in government spaces on government-provided NMCI workstations. At the completion of these tasks, all software and customized computer code shall be surrendered to the Government.

The Government will provide remote access to systems at the NAVFAC Information Technology Center at Port Hueneme, CA to accomplish assigned work covered in this Contract when support effort is not required to be on-site in government spaces. The access will be in compliance with current NETWARCOM, SPAWAR, NMCI and NAVFAC guidance and directives. The Government

EHS PWS

will provide access to any installation required in accordance with current DOD and Navy guidance and directives.

6. Contractor Furnished Information, Services, And Equipment

The Contractor shall provide technical support as needed to meet the requirements of the Contract as it pertains to facilities, supplies and services.

Contractor is responsible for obtaining Card Readers and Software to be utilized with the Government furnished CAC Cards on non-NMCI workstations.

Contractor workstations connecting remotely to the NAVFAC Information Technology Center at Port Hueneme, CA will be in compliance with current NETWARCOM, SPAWAR, NMCI and NAVFAC guidance and directives.

Contractor shall be responsible for reproduction and shipping charges for training manuals.

Contractors traveling overseas shall be required to provide passports.

7. Other Information/Period Of Performance/Travel/ Points Of Contact

7.1. Hours of Work:

Hours of work shall vary based on the task being performed. Certain tasks may require work and travel after normal business hours, on weekends and holidays. For certain tasks, the contractor may be required to provide services 24 x 7. Actual hours of work will be agreed upon at Contract start up

7.2. Place of Performance:

NAVFAC Information Technology Center (NITC)
1000 23rd Avenue, Building 2
Port Hueneme, CA 93043

OR

This Contract work may require work to be performed at any NAVFAC CONUS/OCONUS location, see Attachment 06.

7.3. Period of Performance:

This contract period of performance shall be for one (1) base year and two (2) one-year options and is subject to the availability of Government funds. The option years may be exercised when determined by the Government to be in its best interest and in accordance with applicable acquisition regulations and policies.

In accordance with FAR 52.217-9 Option to Extend the Term of the Contract (Mar 2000), the Government may extend the term of Contract by written notice to the Contractor five (5) days prior to contract expiration provided that the Government gives the Contractor a preliminary written notice of its intent to extend at least 30 days before the contract expires. The preliminary notice does not commit the Government to an extension. If the Government exercises this option, the extended contract shall be considered to include this option clause. The total duration of Contract, including the exercise of any options under this clause, shall not exceed 3 years.

EHS PWS

7.4. Travel:

The contractor shall perform travel as required in the performance of the contract as stated in individual task orders. Travel shall consist of CONUS/OCONUS travel, in support of the contract requirements identified in this Contract.

Travel arrangements and costs shall be in accordance with the Joint Federal Travel Regulations. Before undertaking any travel in performance of this Contract, the Contractor shall have the travel approved, in writing. Any travel expenses that are invoiced to the government shall be accompanied with backup or supporting documents.

7.4.1. Air:

The contractor shall, to the maximum extent practical, minimize overall travel costs by taking advantage of discounted airfare rates available through advance purchase. Charges associated with itinerary changes and cancellations under nonrefundable airline tickets are reimbursable as long as the changes are driven by the work requirement.

7.4.2. Non-Reimbursable Travel:

The following travel shall not be reimbursed: travel performed for personal convenience or daily travel to and from the designated work site.

7.5. Training:

The Government will not allow costs, nor reimburse costs associated with the contractor training employees in an effort to attain and/or maintain minimum personnel qualification requirement nor any specialized certification requirements of this Contract. Attendance at workshops or symposiums and IA certification tests are considered training for purposes of this clause.

7.6. Monthly Status Reports:

The contractor shall submit a monthly status report consisting of an executive summary covering the major activities, burn rates, and financial status of the previous month. These reports shall contain an accurate, up-to-date summary account of major accomplishments completed during the month, actual and projected burn rates (hours and funds), and financial status of the contract. Report will be provided in a PowerPoint presentation. An alternate report may be substituted for this format as agreed to at task start up.

The Contractor shall submit monthly reports in electronic format 5 business days after the previous month.

7.7. NAVFAC IT Hosting Architecture:

Is identified in the NAVFAC Common Operating Environment (Attachment 02).

7.8. Key Positions:

The Contractor agrees to assign full-time equivalent (FTE) personnel to positions designated as key positions and these personnel shall be committed to the project for its duration. No substitution shall be made without prior notification to and concurrence of the Ordering Officer. All proposed substitutes shall have qualifications equal to or higher than the qualifications of the person to be replaced. The Ordering Officer shall be notified in writing of any proposed substitution at least forty-five (45) days, or ninety (90) days when a security clearance is to be obtained, in advance of the proposed substitution. The notification shall include:

- An explanation of the circumstances necessitating the substitution;
- a complete resume of the proposed substitute;

EHS PWS

- and any other information requested by the Ordering Officer to enable the Government to judge whether or the Contractor is maintaining the same high quality of personnel.

Contractor personnel holding the position titles and having the qualifications listed in Attachment 04 are considered essential to the work being performed under this Contract.

7.9. Contractor Identification:

In accordance with DFARS 211.106, "Contractor employees shall identify themselves as contractor personnel by introducing themselves or being introduced as contractor personnel and displaying distinguishing badges or other visible identification for meetings with Government personnel. All contractor employees shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence."

Contractor shall ensure, to the extent practicable, that external correspondence signed by Contractor employees is on company letterhead. Internal correspondence, including e-mail and memoranda, must include the name of the company in the signature line or in another clearly identifiable location. In all contact with the public and Government officials, contractor personnel shall identify themselves as contractor employees working under contract to NAVFAC.

Contractor shall ensure that their onsite personnel, when receiving or placing telephone calls, identify their employer, in addition to whatever other appropriate greeting are used.

When participating in meetings with Government and/or other Contractor employees, ensure that their personnel properly identify themselves as Contractor employees so that their actions will not be construed as acts of Government officials.

All Contractor staff working on-site at any of the client installations during task order performance shall wear at all times a DOD or Contractor furnished Identification.

The Contractor must comply with the implementation of Federal Information Processing Standards (FIPS) Publication Number 201, Personal Identify Verification of Federal Employees and Contractors.

7.10. Intellectual Property:

This Contract is funded by the United States Government. All intellectual property generated and/or delivered pursuant to this Contract shall be subject to appropriate federal acquisition regulations which entitle the Government to unlimited license rights in technical data and computer software developed exclusively with Government funds, a nonexclusive license to practice any patentable invention or discovery made during the performance of this Contract, and a nonexclusive and irrevocable worldwide license to reproduce all works (including technical and scientific articles) produced during this Contract.

All products delivered under this statement of work shall conform to current DOD, Department of Navy (DON) and NAVFAC standards and guidelines. The Navy shall maintain full data rights to all products and deliverables.

7.11. Transition between Contract and Continuity of Service:

If a successor contract is awarded prior to the final expiration date of this Contract, the Government may issue task orders to the successor Contractor prior to the expiration date of this Contract.

EHS PWS

The Contractor must recognize that services under this Contract are vital to the Government and must be continued without interruption and that upon Contract expiration, a successor, either the Government or another Contractor, may continue such services. The Contractor agrees to exercise its best efforts and cooperation to effect an orderly and efficient transition.

The awardee shall not recruit on Government premises or otherwise act to disrupt Government business. Within ten (10) calendar days of a Contract award, the Contractor shall inform the appropriate TOM of incumbent personnel, who will not be placed on the Contract.

The Contractor shall have management and administrative support in place to fulfill work requirements at time of commencement of the Contract performance. Addresses, telephone numbers, and functional responsibilities shall be provided to Ordering Officer and TOM at time of work initiation.

The Contractor shall provide phase-in, phase-out services, at no additional cost to the Government, as long as there is any active Contract. Appropriate Contract management personnel shall meet with the successor Contractor to coordinate Contract transition. Discussions shall include personnel transition to the successor Contractor, and the transition of Contract specific items such as Government or Contractor furnished supplies, materials, equipment, and services.

The Contractor shall disclose necessary personnel records (names and phone numbers) to allow the successor to conduct interviews for possible transition. If selected employees are agreeable to the change, the incumbent Contractor shall grant release at a mutually agreed date and negotiate transfer of the employee's earned fringe benefits. The resumes for incumbents must be approved by the Government prior to assignment to a position.

EHS PWS

8. Attachments

Attachment 01 - Enterprise Business Systems

P L A C E H O L D E R

EHS PWS

Attachment 02 - Common Operating Environment (COE)

P L A C E H O L D E R

EHS PWS

Attachment 03 - Application Technology Stacks and Hosting Services

P L A C E H O L D E R

EHS PWS

Attachment 04 - Key Positions

P L A C E H O L D E R

EHS PWS

Attachment 05 - Non Disclosure Form

P L A C E H O L D E R

EHS PWS

Attachment 06 - Department of Homeland Security Employment Eligibility Verification, Form I-9

P L A C E H O L D E R

EHS PWS

Attachment 07 - Contractor Verification System (CVS)

P L A C E H O L D E R

EHS PWS

Attachment 08 - System Authorization Access Request Form (SAAR)

P L A C E H O L D E R

EHS PWS