NAVFAC
ENTERPRISE OPERATIONS SUPPORT SERVICES (EOS) PERFORMANCE WORK STATEMENT (PWS)

VERSION 2

8/18/2011

EOS PWS V2

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: 5
1.2.2. Privacy Act: 6
1.2.3. Access Requirements: 7
1.3. Physical Security 7
1.4. Background: 8
1.5. Objective: 8
2. Definitions as applied to this contract 8
2.1. Common Operating Environment (COE) 8
2.2. Defective Service 9
2.3. Continuous Process Improvement (CPI) 9
2.4. Government-Approved Outages 9
2.5. Contracting Officer's Representative (COR) 9
2.6. Quality Control (QC) 9
2.7. Quality Assurance (QA) 9
2.8. Knowledge and Skill Levels 9
2.9. Government and Acquisition Acronyms 10
2.10. Information Technology and Information Assurance Acronyms 11
2.11. References 12
3. Enterprise Operations Services (EOS) Contract Description And Deliverables 13
3.1. NITC Service Desk Support 13
3.1.1 Incident Management Support 13
3.1.2 Process Monitoring Support 14
3.1.3 Event/Incident Notification Support 14
3.1.4 Inventory and Asset Control Support 14
3.1.5 Facility Management and Physical Security Support 15
3.1.6 Office and Reception Duties 15
3.2 Local Operations Support and Help Desk 16
3.2.1 Navy Marine Corps Intranet (NMCI) Continuity of Service Contract (COSC) Support 17
3.2.2 Cyber Asset Reduction and Security (CARS) Support 18
3.3 Information Assurance (IA) 19
3.3.1 Information Assurance Certification and Accreditation (C&A) Support 19
3.3.2 Information Assurance Compliance and Audit Support 20
3.3.3 Information Assurance Continuity and Recovery Planning Support 21
3.3.4 Information Assurance Certification and Accreditation Technical Writing Support 22
3.3.5 Information Assurance Security Technical Implementation Guide (STIG) 23
3.4 Continuous Process Improvement and Quality Assurance 25
3.4.1 Data and Document Management 25
3.4.2 Change Management 25
3.4.3 Configuration Management (CfM) 26
3.4.4 Quality Assurance 27
3.4.5 Portfolio Management 28
3.4.6 Information Technology Infrastructure Library (ITIL) 29
3.5 End-to-End (E2E) Performance Management Support 30
3.5.1 End-to-End Performance Management 30
3.6 Project Management 31
3.6.1 Project Management and Planning 31
3.6.2 Status Reports and Meetings 31
3.6.3 Program Oversight 32
3.7 Performance Requirements Summary Matrix 33
3.8 Deliverables 42
4. Quality Planning, Control And Assurance 44

EOS PWS V2

5. Government Furnished Information, Services, And Equipment....44
6. Contractor Furnished Information, Services, And Equipment....45
7. Other Information/Period Of Performance/Travel/ Points Of Contact....45
7.1 Hours of Work:....45
7.2 Period of Performance:....45
7.3 Travel:....46
7.3.1 Air Travel:....46
7.3.2 Non-Reimbursable Travel:....46
7.4 Training:....46
7.5 Monthly Status Reports:....46
7.6 Contractor Identification....47
7.7 Intellectual Property:....47
7.8 Transition between Contract and Continuity of Service:....47
Appendices....49
Appendix A - References and Publications....49
Tables....50
Table 01 - Help Desk Support Services and IAT Level Requirements....50
Attachments....52
Attachment 01 - Enterprise Business Systems....52
Attachment 02 - Common Operating Environment (COE)....53
Attachment 03 - Non Disclosure Form....54
Attachment 04 - Department of Homeland Security Employment Eligibility Verification, Form I-9....55
Attachment 05 - Contractor Verification System (CVS)....56
Attachment 06 - System Authorization Access Request Form (SAAR)....57

EOS PWS V2

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 operational and technical support to include deployment support, operations and maintenance, configuration management, change management, project management, planning and analysis, and information assurance support for all NAVFAC Enterprise Business Systems hosted at NITC. The focus of this task order is the provisioning of day-to-day operational support, customer liaison, change and configuration management, information assurance, life cycle management, portfolio and asset management, quality assurance, validation and verification, business continuity, facilities management, documentation, and process improvement .

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. The Enterprise Operations Support (EOS) provides the necessary administration, planning, coordinating and testing of the business contingency plan for continuity of operations. In collaboration with the NITC NASP and CDA resources, the EOS ensures that regular testing is conducted and results are reported to management.

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

POSTPWS V2

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 NITC Team, and the Central Design Agency (CDA), the Contractor shall determine the best approach for meeting IA and FISMA compliance without impacting business systems availability and performance.

Continuous process improvement (CPI) and standardization using the ITIL framework is a major initiative at NITC. Although several operational processes are now in place at NITC, these processes need to be continually reviewed, audited, tested and maintained to ensure compliance with the latest technological changes, industry best practices, and DON/DOD mandates. Work includes identifying areas for improvement, documenting processes, communicating processes prior to implementation, and continuous improvement using various CPI methodologies.

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

- Recurring support for day-to-day systems operations which include: system provisioning, system monitoring and reporting, help desk level 1 troubleshooting and technical support, service request management and tracking, maintenance coordination, facility monitoring.

- Security compliance and accreditation support for all business systems listed in Attachment 01 including the two accredited network enclave packages. This includes but not limited to: continuous review of systems and network accreditation packages, monitoring plan of action and milestones (POA&M) completion, security scan output reviews, vulnerability reviews and mitigation actions and reporting, DIACAP packages review and processing, INFOCON report management, FISMA compliance reports.

- Standardization and Continuous process improvement utilizing ITIL framework which include: change management, configuration management, quality assurance reviews and audits, portfolio and asset management, life cycle management, license management, and technical process documentations.

- Administration of the business continuity plan and continuity of operations initiatives (BCP/COOP). This includes developing project plans, coordinating, communicating and implementing testing plans without impacting normal business systems operations.

- Providing remote technical support, operations, and sustainment of all mainframe systems hosted at DISA Mechanicsburg and Ogden

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

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.

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 NAVFAC Business Systems. 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

EOS PWS V2

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 03).

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 05 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. . This and other government -mandatory trainings will occur at Government's expense.

Contractor employees shall fill out a System Authorization Access Request Form (SAAR) to obtain access to any Government system (remote or otherwise), see Attachment 06

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. Physical Security

The Contractor shall be responsible for safeguarding all Government property provided for Contractor use. At the close of each work period, Government facilities, equipment, and materials shall be secured in accordance with federal, DoD, DON, and local policy requirements.

The Contractor shall establish and implement methods of making sure all keys/key cards issued to the Contractor by the Government are not lost or misplaced and are not used by unauthorized persons.

EOS PWS v2

1.4. 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, associates, and employees. The NAVFAC Information Technology Center (NITC) serves as NAVFAC's primary Information Technology Service Provider, offering a wide variety of technical solutions and support to the NAVFAC organization. The NITC organization is divided into the following areas of responsibility:

- Central Design Agency (CDA) – provides software solutions development and system engineering.
- NAVFAC Application Services Provider (NASP) – provides the overarching technological support for the hosting infrastructure in support of all Enterprise Business Systems hosted at NITC.
- Enterprise Operations and Information Assurance (EOIA) – provides Enterprise Operational support, Information Assurance support, and Independent Verification and Validation (IV&V) 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 Support (EBS-COTS), Enterprise Business Support Non-Commercial Off-the-Shelf (EBS-NonCOTS) Support and Enterprise Hosting Support (EHS).

1.5. Objective:

The objective of this acquisition includes implementing and employing enterprise operational support processes for the NAVFAC business systems, including information assurance, process documentation, configuration management, quality assurance, independent verification and validation, collaborative review, customer support, and problem resolution.

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.

EOS PWS V2

2.2. Defective Service

A service output that does not meet the standard of performance associated with it in the Performance Work Statement

2.3. 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.

2.4. 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.

2.5. Contracting Officer's Representative (COR)

A COR is a Government employee that serves as a liaison to the Contractor and provides surveillance functions.

2.6. Quality Control (QC)

Actions taken by the Contractor to control the quality (performance) of services, ensuring requirements of the PWS are met.

2.7. Quality Assurance (QA)

Actions taken by the government to ensure Contractor services meet the requirements of the PWS.

2.8. 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

EOS PWS-V2

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.

2.9. Government and Acquisition Acronyms

Acronym	Description
ACNO-IT	Assistant Chief of Naval Operations for Information Technology
ACTR	Assistant Contract Technical Representative (NMCI terminology)
ANACI	Access National Agency Check with Inquires
AQL	Acceptable Quality Level
ASDP	Abbreviated Systems Decision Paper
B2B	Business to Business
BCA	Business Case Analysis
BOY	Beginning of (Fiscal) Year
CAC	Common Access Card
CCB	Configuration Control Board
CCR	Central Contractor Registration
CEC	Civil Engineering Corps
CLIN	Contract Line Item Number
CNO	Chief of Navy Operations
COB	Close Of Business
CONUS	Continental United States
COR	Contracting Officer's Representative
CoS	Continuity of Service
CPI	Continuous Process Improvement
CTR	Contract Technical Representative (NMCI terminology)
CVS	Contractor Verification System
CYE	Calendar Year End
DFAR	Defense Federal Acquisition Regulation
DISA	Defense Information Systems Agency
DoD	Department of Defense
DODD	Department of Defense Directive
DODI	Department of Defense Instruction
DON	Department Of Navy
DSS	Decision Support System
DWAS	Defense Working capital fund Accounting System
E2E	End to End
EOY	End Of (Fiscal) Year
EP	Execution Plan
FAM	Functional Area Manager
FAR	Federal Acquisition Regulation
FAQ	Frequently Asked Questions
FEC	Facilities Engineering Command
FMO	Financial Management Office
FTE	Full-Time Equivalent
FY	Fiscal Year
GF	General Fund
GOTS	Government-off-the-shelf
HVAC	Heating, Ventilation and Air Conditioning
IPT	Integrated Product Team
JPAS	Joint Personal Adjudication System

EOS PWS V2

NACLA	National Agency Check with Local Agency
NAVFAC	Naval Facilities Engineering Command
NBVC	Navy Base Venture County
NGEN	Next Generation NMCI Network (see NMCI)
NAVNETWARCOM	Naval 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
OCONUS	Outside Continental United States
ONE-NET	OCONUS Navy Enterprise Network
OO	Ordering Officer
OST	Operational Support Team
PBSOW	Performance Based Statement of Work
PEO-EIS	Program Executive Office for Enterprise Information Systems
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	Quality Improvement (as applicable to QI Sessions)
RFA	Request for Action
ROI	Return on Investment
SECNAV	Secretary of the Navy
SDP	System Decision Paper
SLIN	Sub Line Item Number
SSBI	Single-Scope Background Investigation
TOM	Task Order Manager
TRM	Total Resource Management
TSO	Time Sharing Option
USC	US Code (US Public Law)

2.10. Information Technology and Information Assurance Acronyms

Acronym	Description
AHF	Application Hosting Facility
ATL	Automated Tape Library
BCP	Business Continuity Plan
BMS	Business Management System
BPM	Business Process Monitor (performance monitoring software)
C&A	Certification and Accreditation
CA	Certification Agent
CCM	Configuration & Change Management
CCMP	Configuration & Change Management Plan(s)
CDA	Central Design Agency
CIAM	Command Information Assurance Manager
CIO	Command Information Officer
CM	Configuration Management
CMMI	Capability Maturity Model Integration

EOS PWS V2

CMP	Configuration Management Board
COE	Common Operating Environment
COOP	Continuity of Operations Plan
COTS	Commercial-off-the-shelf
DAA	Designated Approval Authority
DADMS	DON Applications and Database Management System
DBMS	Database Management System
DECC	Defense Enterprise Computing Center
DIACAP	DoD Information Assurance Certification and Accreditation Process
DRP	Disaster Recovery Plan
FISMA	Federal Information Security Management Act
IA	Information Assurance
IAM	Information Assurance Manager
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IAWF	Information Assurance Work Force
INFOCON	Information Operations Condition
IT	Information Technology
ITIL	Information Technology Infrastructure Library
IV&V	Independent Verification and Validation
NAS	Network Attached Storage
NASP	NAVFAC Application Service Provider
ODAA	Operational Designated Approval Authority
OS	Operating System
PKE	Public Key Enabling
PKI	Public Key Infrastructure
POA&M	Plan of Actions and Milestones
QTP	Quick Test Professional
SAAR	System Authorization Access Request
SAN	Storage Area Network
SCADA	Supervisory Control and Data Acquisition
SRR	System Readiness Review
SSL	Secure Sockets Layer
STIG	Security Technical Implementation Guide(s)
T&E	Test & Evaluation (applicable to C&A requirements)
TPS	Test Plan/Script
TR	Technology Refresh
TS	Technology Stack
UPS	Uninterrupted Power Supply

EOS PWS V2

2.11. References

Select publications applicable to this PWS are listed in Appendix A. Electronic copies of all applicable documents and publications will be provided by the Work Requestor upon request.

3. Enterprise Operations Services (EOS) Contract Description And Deliverables

Overview: This task order consists of implementing, managing, or executing various support processes for the NAVFAC Enterprise Business Systems (EBSs). Services required are as follows:

- Implement and operate help desks, local operation, and IT services
- Provide information assurance support services
- Develop and validate continuity of operations plans
- Implement and provide oversight of configuration and change management support processes
- Implement and manage a program for independent verification and validation of quality assurance
- Provide support services for the Navy's Cyber Asset Reduction and Security (CARS) initiatives

3.1. NITC Service Desk Support

Overview: The Contractor shall implement and maintain a 24 x 7x 365 on-site operations desk at NITC Port Hueneme, CA. The Contractor shall work with NAVFAC to understand and support business and organization requirements and translate those into processes and procedures that assist the contactor in managing the Service Desk and Customer Support function for the enterprise. The Contractor shall proactively review, maintain, disseminate, and improve NITC Service Desk procedures.

3.1.1 Incident Management Support

Work Description: The Contractor shall perform the following tasks:

- Operate the Customer Support Desk.
- Accept and log calls from users. Receive, analyze, resolve, escalate, and coordinate the resolution of issues. Follow-up with customers, when needed.
- Document user and facility issues in the tracking system.
- Provide accurate metrics relating to quantity, category, status, and resolution of issues. Customer service complaints to total tickets handled cannot exceed 3%, based on feedback. Issues defined as incidents will be reviewed for timely responses and adherence to documented ticket management practices. Outstanding incidents that have not been resolved within a reasonable amount of time will be prime candidates for review (to include aging 30, 60, and 90 day tickets). Government review of outstanding incidents and a random sample of service desk trouble tickets must show at least 95% contain complete detailed information: customer contact information, end-user symptoms, end-user account information, troubleshooting method, justification for escalation to an SME (if applicable), and follow-up contact to confirm resolution of issue (if applicable).

Objectives:

A. Provide courteous, efficient and timely responses to all customers..
B. Receive, analyze, resolve, escalate and coordinate the resolution of user issues.

Deliverables:

0001 - User Issues Metrics

EOS PWS V2

3.1.2 Process Monitoring Support

Work Description: The Contractor shall perform the following tasks:

- Monitor NAVFAC business systems, servers, and service availability and performance.
- Monitor NITC hosted applications, DISA mainframe applications, and NITC facility and designated equipment and detection systems.
- Acknowledge, log, and resolve issues, in a timely manner, as defined by the procedures set forth for each monitoring system. Procedures will be reviewed for accuracy on a regular and reoccurring basis.
- Review, update, and maintain Operations Watch procedures, in conjunction with government representatives, on a quarterly basis. As proof of acceptable quality, both Operations Watch and the government representative will formally acknowledge or sign for the successful completion of a procedure review or update.

Objectives:

A. Monitor NITC hosted applications, DISA mainframe applications and the NITC facility.
B. Review and maintain NITC Operations Watch procedures

Deliverables:

0002 - Up-to-date NITC Operations Watch Procedure

3.1.3 Event/Incident Notification Support

Work Description: The Contractor shall perform the following tasks:

- In conjunction with a designated Government representative, Operations Watch will review, update, and maintain procedures, on a quarterly basis,
- Information will accurately reflect the status of issues and be provided in accordance with agreed upon formats and timeframe.

Objectives:

A. Document operational status, application and facility issues and share information as required to NAVFAC users and management
B. Provide reports and metrics to NAVFAC management regarding operational status and support issues.
C. Communicate and coordinate with NAVFAC CIO Help Desks across NAVFAC organizations worldwide and provide standard operating procedures and policies for use by the NAVFAC Help Desk community

Deliverables:

0003 - Operations status report

3.1.4 Inventory and Asset Control Support

Work Description: The Contractor shall perform the following tasks:

- Provide support for tracking NITC property and assets. Receive, remove, and inventory all property and assets. Software distribution and tracking support will be provided during non-core business hours. Destruction and removal of equipment shall be done following standard federal, local, and DoD procedures.
- Provide video conferencing support arrangements via the Support Tracking System (STS) process and direct audio conferencing support.

FOUO PWS V2

- Secure and log all assets into Defense Property Accountability System (DPAS). All staff assigned to this area must have appropriate training, certification, and access to DPAS. All data center hardware will be accounted for in DPAS. Accurate accounting and reporting of all inventories in a data center will be accomplished on a regular basis (yearly minimum) or as requested.

Objectives:

A. Provide video conferencing support arrangements via ticketing system process and direct audio conferencing support.
B. All data center hardware and assets are secured and accounted for in the DPAS.
C. Destruction and removal of equipment shall be done in accordance with federal, state, local and DoD guidance.
D. Maintain and update processes and procedures for managing inventory.
E. Staff must have access to DPAS system

Deliverables:

0004 - Up-to-date asset inventory in DPAS

3.1.5 Facility Management and Physical Security Support

Work Description: The Contractor shall perform the following tasks:

- Monitor, initiate action to resolve, and report issues related to NITC facility environmental control alarms/alerts (security, surveillance, fire, power, HVAC, halon and water detection).
- Provide support developing and granting appropriate access to facility and assets and maintain building entry system, security alarms, and surveillance equipment and monitoring. The Contractor will defend against unauthorized access to facility, assets, systems, networks, and data.
- Log and communicate all access issues with the NAVFAC Facility Manager.

Objectives:

A. Provide support in maintaining building entry system, security alarms, surveillance equipment and monitoring.
B. Provide support in developing and granting appropriate access to facility and assets including hardware and software.

3.1.6 Office and Reception Duties

Work Description: The Contractor shall perform the following tasks:

- Provide general office and reception duties: answer and route phone calls, draft, send, and respond to emails, provide visitor services (issue badges, give directions, etc.).
- Use Microsoft Office suite to accomplish duties, as required.

Objectives:

A. Greet visitors and provide directions and guidance to various locations in the facility and provide information about the facility and personnel to authorized guests.
B. Ensure visitors are easily identifiable.

Deliverables:

0005 - Completed Visitors Log

EOS PWS V2

3.2 Local Operations Support and Help Desk

Overview: The Contractor shall provide technical and administrative systems support services for standard, common, migrations or systems. IA certification requirements are based on the SECNAV M-5329.2. Information Assurance Technical (IAT) Level I certification is required for certain types of support. The certification level will be detailed on specific work requests.

Work Description: The Contractor shall perform the following tasks:

- Provide technical and administrative systems operation support services for standard, common, migrations or systems.
- Develop, maintain and revise existing operations schedules for daily and other regularly scheduled data transfers and updates.
- Monitor job schedules and their execution status.
- Provide technical and operations support for the unclassified messaging system.
- Provide assistance with the scheduling and set-up of Video Teleconferences (VTC) and Training rooms. Some requests may require coordination with the enterprise. Provide conference lines for attendees connecting via telephone.
- Manage, track and operate a loan pool of equipment for use by traveling employees or other offsite use.
- Provide a COSC Science and Technology (S&T) configuration manager. The S&T CfM is responsible for providing configuration support to the end-user for these workstations.
- Coordinate software installation with end users, or install software for end users as required.
- Assist end users with administrative requirements of associated S&T community of interest (COI), including assistance with forms, software configuration, licensing and inventory control.
- Provide general end-user and legacy application help desk support, including requests received via phone, email, walk-up, or submission by an automated trouble tracking tool. The help desk shall capture and document problems and solutions using NAVFAC software.
- Track the resolution of user problems, keeping the user informed of progress. Follow-up with the user after problem.
- Provide technical and operations support for sanction desktop applications such as the Microsoft Office.
- Assist with the installation of government owned peripherals devices on COSC workstations.
- Provide end-user liaison support for accessing network (NMCI) services.
- Manage distribution lists that are maintained on NMCI.
- Assist users in tasks that allow for a more efficient operation of their desktop system.
- Provide end-user support, including configuration assistance, for various software applications used by the activity.
- Manage kiosk machines. Coordinate software installation with end users, or install software for end users as required. Assist end users with administrative requirements of any required forms, software configuration, software licenses and inventory control.
- Maintain the Field Help Desk Documentation. This documentation shall include technical manuals, trouble tracking tool, help desk knowledge base and standard

EOS PWS V2

Field Operations/Help Desk procedures. The Contractor shall submit changes for review and acceptance by the government.

Objectives:

A. Provide operations support.
B. Provide S&T seat configuration management.
C. Insure calls are answered promptly by operations/help desk personnel.
D. Time to resolve user problems or answer question is as short as possible.
E. Operations/help desk personnel are courteous and efficient.
F. Maintain operations/help desk documentation.

Deliverables:
0006 - Up-to-date Operations & HelpDesk procedures

3.2.1 Navy Marine Corps Intranet (NMCI) Continuity of Service Contract (COSC) Support

Overview: Navy Marine Corps Intranet (NMCI) Continuity of Service Contract (COSC) Program, via contract to Hewlett Packard (HP), provides IT network and desktop PC seat services to the Department of the Navy. The Department of the Navy provides the strategic direction for the program. HP provides services delivery. Both the Navy and HP provide operational direction, via electronic orders, help desk requests, and other change requests.

NAVFAC requires Contractor support services for a COSC Customer Technical Representative (CTR), located at headquarters, or a COSC Activity Customer Technical Representative (ACTR) located at field activities. This support includes coordinating the acquisition and implementation of local seat management activities. Some work performed under this task will require IA certification.

Work Description: The Contractor shall perform the following tasks:

- Support and monitor COSC Move-Adds-Changes (MAC) at either an enterprise (CTR) or a local activity (ACTR). These MACs include applications configuration changes, hardware changes, account changes, ramifications of personnel moves and transfers, and other operational change ordering and tracking.
- Review and submit MAC requests.
- Provide MAC projections for current and out year requirements.
- Use the NMCI COSC ordering and asset management tools to acquire COSC services and manage the inventory of COSC provided assets.
- Setup and maintain new service request management groups.
- Coordinate the scheduling of COSC system delivery and refresh efforts.
- Identify and resolve issues related to transition and sustainment activities with the COSC contractor, the Navy Program Management Office, and NAVFAC activity components.
- Provide administration of user accounts for NMCI.

Objectives
A. Support and monitor MACs at an enterprise level..
B. Provide MAC projections for current and out year requirements.
C. Setup and maintain new service request management groups.

EOS PWS V2

Deliverables:
0007 - MAC List (current and projected)

3.2.2 Cyber Asset Reduction and Security (CARS) Support

Overview: The Navy is undertaking major efforts to reduce its IT footprint and costs. One of these efforts is the Cyber Asset Reduction and Security (CARS) project. CARS will improve Navy enterprise-wide IT security, interoperability, return on investment (ROI), and provide ashore information technology (IT) (secret and below) asset visibility (cost, configuration and accountability) in preparation for post-NMCI COSC environment in fiscal year 2014. Contractor resources shall be required to support the various stages of this initiative

Work Description: The Contractor shall perform the following tasks:

- Apply the policies outlined in the NMCI Continuity of Service Contract (COSC) Legacy Systems Transition Guide, Legacy Network Shutdown (LNS) Solutions Matrix, updated guidance from the CARS Task Force (TF), NMCI COSC LNS IPT, NAVNETWARCOM, and other sources to determine feasible solution alternatives, estimate resource requirements, and recommend solutions for legacy network components. These solutions may include use of various COSC contract CLINs.
- Work with NAVFAC, Navy, and HP personnel to implement the solutions, including development of COSC unpriced CLIN documents. Implementation may involve adapting to and resolving various configuration management issues.
- Work with NAVFAC IT staff, including application managers, to organize production and submission of C&A documents and testing as required to meet current NAVNETWARCOM and Program Executive Officer, Enterprise Information Systems (PEO-EIS) requirements for systems transition to NMCI COSC and ONE-NET.
- Support NAVFAC activities' legacy network decommissioning. The Contractor shall determine that a legacy network component can be shutdown without negative mission impact and confirm the shutdown so that government resources are no longer connected to a legacy network.
- Document templates and processes developed in the course of the CARS support effort so that NAVFAC can repeat the processes as necessary during (and if necessary, after) the completion of the legacy network reduction, ITFMR, and IAM tool deployment work.

Objectives:
A. Migration solutions identified.

EOS PWS V2

3.3 Information Assurance (IA)

3.3.1 Information Assurance Certification and Accreditation (C&A) Support

Overview: The tasks completed under this order shall provide analytical, technical and documentation support to NAVFAC for supporting C&A efforts, ensuring the command implements Information Assurance standards, policies, and objectives as defined in SECNAVINST 8500.1, 8500.2 and other DoD and DON related policies. All documents are to be in formats as directed by IA policy and guidance.

In accordance with Information Assurance Work Force (IAWF) requirements as detailed in DoD 8570.01M and SECNAV M-5239.2, Contractor resources supporting this task order are required to hold and maintain IA certification for Information Assurance Manager (IAM) Level I. The Contractor shall pay for all training, study time, exam, and certification. Contractors/vendors shall encourage employees to pursue IT certifications relative to the work performed.

Work Description: The Contractor shall perform the following tasks:

- Provide Information Assurance Certification and Accreditation (C&A) support in accordance with all applicable DoD and DON guidance. The contractor shall perform security risk assessments that are focused on the measurement of compliance to ensure the availability, integrity, identification, authentication, confidentiality, and non-repudiation of friendly information and Information Systems while denying adversaries access to the same information and Information Systems.
- Coordinate with Government IA functional managers to support Information Assurance requirements as directed by CNO, NAVNETWARCOM, and NAVFAC. This includes support to the Navy's IA DITSCAP/DIACAP certification and accreditation (C&A) requirements as defined in policies and guidance. The contractor will interface with NAVFAC application owners and IA management to facilitate the updating of application C&A packages and perform required DIACAP Test and Evaluation (T&E) efforts in accordance with application guidance and policy.
- Participate in the completion of C&A documents for hosted applications and hosting environments. The Contractor shall review, maintain, and disseminate information relating to NITC/NAVFAC C&A procedures and business processes. The Contractor shall participate in improving C&A business processes used by the IA team. Tasks will include performing Risk Analysis related to IA/C&A compliance, providing recommendations on mitigations in support of C&A requirements, and preparing Plans of Action and Milestones (POA&Ms) in support of risk mitigation efforts.
- Coordinate with Government IA functional managers to support Information Assurance requirements as directed by CNO, NAVNETWARCOM, and NAVFAC. This includes support to the Navy's IA DITSCAP/DIACAP certification and accreditation (C&A) requirements as defined in policies and guidance.
- Interface with NAVFAC application owners and IA management to facilitate the updating of application C&A packages.
- Perform compliance testing for DIACAP IA Controls as applicable to Information System MAC and Confidentiality Level (CL) requirements; namely, conducting Test and Evaluation (T&E) events, working with Information System owners and their representatives, documenting the results, providing recommendations as the Subject Matter Expert (SME), and compiling all required information and artifacts into a comprehensive DIACAP package .
- Provide Information Assurance (IA) risk analysis and risk mitigation support to include categorization of initial risk and residual risk as well as impact if risk is exploited. Risk mitigation support shall include development of courses of action recommendations, associated timelines, and implementation support for the NAVFAC Application Service Provider (NASP) and Central Design Agency (CDA) divisions as required.

FOUO Pages V2

- The contractor shall work closely with Configuration and Change Management (CCM), Business Continuity, and IA teams to coordinate and document changes that affect C&A documentation packages.

Objectives

A. Implement and coordinate IA C&A business processes.
B. Prepare and coordinate the efforts associated with completing C&A documents in support of applications and hosting environments.
C. Ensure C&A documents are updated as changes are implemented.

Deliverables:

0008 - Fully maintained C&A documents
0009 - Up-to-date IA C&A business processes

3.3.2 Information Assurance Compliance and Audit Support

Overview: The tasks completed under this order shall provide analytical, technical and documentation support to NAVFAC for supporting C&A efforts, ensuring the command implements Information Assurance standards, policies, and objectives as defined in SECNAVINST 8500.1, 8500.2 and other DoD and DON related policies. All documents are to be in formats as directed by IA policy and guidance.

In accordance with Information Assurance Work Force (IAWF) requirements as detailed in DoD 8570.01M and SECNAV M-5239.2, Contractor resources supporting this task order are required to hold and maintain IA certification for Information Assurance Manager (IAM) Level I. Contractors/vendors shall encourage employees to pursue IT certifications relative to the work performed.

Work Description: The Contractor shall perform the following tasks:

- Participate in the completion of IA Compliance documents for hosted applications and hosting environments; particularly, Plan of Action and Milestones (POA&M) documents.
- Assist the site in eliminating/reducing/mitigating system and network vulnerabilities to an acceptable severity category level as defined by DoD 8510.01 and NIST 800-30. This effort will prepare NAVFAC business systems for the DIACAP Test and Evaluation (T&E) necessary to receive and maintain Authority to Operate (ATO).
- Identify and provide remediation guidance for technical and non-technical weaknesses found on NAVFAC Information Systems.
- Perform risk analysis and provide recommendations on Information System vulnerability mitigations in support of C&A requirements. Documents are to be in formats as directed by IA policy and guidance. Prepare and provide Plans of Action and Milestones (POA&Ms) in support of risk mitigation efforts.
- Use IA automated assessment tools such as eEYE RETINA, Defense Information Systems Agency (DISA) Gold Disk, Security Readiness Review (SRR) evaluation scripts, and DISA Security Checklists to verify comprehensive and complete implementation of security requirements. Additionally, the Contractor will evaluate the security posture of NAVFAC Information Systems by performing risk assessments through testing of applicable IA Controls for assigned Mission Assurance Category (MAC) and Confidentiality Level (CL).
- Repeat the above-mentioned security risk assessments and procedures periodically to ensure all technical and non-technical vulnerabilities are identified and addressed in a

EOS PWS V2

timely manner. The objective is to eliminate or reduce/mitigate vulnerabilities, maintain IA compliance, and to ensure the continued Confidentiality, Integrity, and Assurance of all NAVFAC Information Systems.

- Review and assess NAVFAC enclave security policies, such as comparing Group Policy Objects (GPOs) settings against Defense Information Systems Agency (DISA) Gold Disk and Security Technical Implementation Guide (STIG) setting standards.
- Audit IA implementation compliance through periodic testing and verification of scanning, patching, and other security updates and configuration settings for all NAVFAC Information Systems.

Objectives

A. Implement and coordinate IA compliance business processes.
B. Prepare and coordinate the efforts associated with IA compliance determinations for all business systems.
C. Ensure IA compliance is maintained and documented.
D. Manage server scan results and vulnerabilities.
E. Perform periodic IA compliance auditing, ensuring results are documented and reported within two (2) business days.

Deliverables

0010 - Up-to-date IA compliance business processes
0011 - IA Compliance Audit Reports
0012 - IA Scan Results and Vulnerabilities Reports

3.3.3 Information Assurance Continuity and Recovery Planning Support

Overview: Information Assurance continuity and recovery planning support represents a broad scope of activities designed to sustain and recover critical IT services following an emergency. This task order will support the Business Continuity Plan (BCP), Continuity of Operations Plan (COOP), Contingency Plan (CP), and Disaster Recovery Plan (DRP).

The Business Continuity Plan provides procedures for sustaining essential business operations while recovering from a significant disruption and the Continuity of Operations Plan provides procedures and capabilities to sustain an organization's essential, strategic functions at an alternate site. The Contingency Plan provides procedures and capabilities for recovering a major application or general support system, and the Disaster Recovery Plan provides detailed procedures to facilitate recovery of capabilities at an alternate site.

Work Description: The Contractor shall perform the following tasks:

- Support contingency, continuity, and disaster recovery planning requirements, ensuring that recovery efforts for the command meet IA standards, policies, and objectives as defined in SECNAVINST 8500.1, SECNAVINST 8500.2 and other DoD and DON related policies.
- Maintain an acceptable level of recovery capability compliance under the direction of the Information Assurance Manager (IAM) or government management.
- Research current applicable BCP, COOP, CP, and DR processes and policies and improve or develop new processes in the area of BCP/COOP compliance, tracking, and maintenance.
- Provide the necessary technical resources to support application and environmental recovery validation and testing requirements.

EOS PWS V2

- Evaluate and report BCP/COOP compliance findings to client representatives and management.
- Assist in the adjudication of negative findings and develop mitigation plans for compliance or Operational Designated Accrediting Authority (ODAA) acceptance of non-compliance.

Objectives

A. Develop and maintain Business Recovery processes documentation.
B. Manage project efforts for full implementation of an Alternate Site facility in collaboration with the NASP technical project manager.
C. Develop and maintain processes related to Recovery execution.
D. Perform annual Contingency and Incident Reponses (CIR) tests and report results.
E. Provide business recovery solution recommendations.

Deliverables

0013 - Business Recovery Process Document
0014 - Business Recovery Testing Plan
0015 - Annual Contingency and Incident Reponses (CIR) Test Reports

3.3.4 Information Assurance Certification and Accreditation Technical Writing Support

Overview: The NAVFAC IA program requires the creation of technical documentation. The type of documentation will be determined based on the individual system and customer need. The government will provide Subject Matter Expert (SME) support, as deemed necessary.

The tasks completed under this order will provide Information Assurance policy support to NAVFAC with respect to federal, DoD, and DON IA related data calls and IA related taskers. All documentation will be designed using standard NAVFAC tools and capable of being printed or deployed via the NAVFAC portal or the Navy network.

Work Description: The Contractor shall perform the following tasks:

- Create target audience specific technical documentation, in a variety of subject areas, to explain complex technical requirement s or capture existing processes.
- Prepare and maintain IA policy documents. The Contractor will provide IA-centric technical writing support to the Information Assurance (IA) Branch and be responsible for authoring, updating, and maintaining all Information Assurance and Certification and Accreditation (C&A) technical documents. The Contractor shall provide expertise in the application of Navy correspondence and documentation standards, practices, methods, and procedures in producing and maintaining IA documentation, records, and publications.
- Prepare documentation required to develop comprehensive DIACAP packages and associated artifacts. As required, test objectives, procedures, and methods shall be defendable both orally and in writing.
- Draft IA policy reviews and data call responses.
- Assist in the collection of test results and data generated during the DIACAP Test and Evaluation (T&E) process.
- Create and maintain detailed IA compliance status and technical reports.
- Develop and maintain reports to track metrics for day-to-day IA operations.
- Create and maintain IA project plans and timelines.
- Maintain certification and accreditation documentation for all NAVFAC Information Systems.

EOS PWS V2

- Participate in IA policy related review boards, integrated process teams (IPTs), and related groups on behalf of NAVFAC IA government officials, when requested. The Contractor shall participate in and document C&A events such as planning sessions, DIACAP package review teams, test and evaluation working groups, and other IA or C&A meetings, as required.

Objective

A. Provide technical writing support for NAVFAC IA and C&A documentation.
B. Develop weekly IA status reports to track IA and C&A metrics.

Deliverables

0016 - Completed IA and C&A Packages
0017 - Weekly IA & C&A Tracking Reports

3.3.5 Information Assurance Security Technical Implementation Guide (STIG)

Overview: The Security Technical Implementation Guide (STIG) provides background and context for access control issues including the process of identification, authentication, and authorization for access to protected assets. The STIG presents a practical methodology for selecting and integrating logical and physical authentication techniques while tying the solution to the asset's value, environment, threat conditions and operational constraints.

In accordance with Information Assurance Work Force (IAWF) requirements as detailed in DoD 8570.01M and SECNAV M-5239.2, Contractor resources supporting this task order are required to hold and maintain IA certification for Information Assurance Level IIII. Contractors/vendors shall encourage employees to pursue IT certifications relative to the work performed.

Work Description: The Contractor shall perform the following tasks:

- Coordinate with Government IA functional managers to support Information Assurance requirements as directed by CNO, NAVNETWARCOM, and NAVFAC. This includes support for DoD STIG requirements.
- Participate in the initial development and completion of STIG documents for hosted applications and hosting environments. The Contractor shall review, maintain and disseminate information relating to NITC/NAVFAC STIG procedures and business processes.
- Participate in improving STIG business processes used by the IA team.
- Interface with NAVFAC application owners, developers, hosting staff, and IA management to facilitate the updating of STIG documentation.
- Perform risk analysis and provide recommendations on mitigations in support of STIG requirements. Documents are to be in formats as directed by IA policy and guidance. The contractor shall prepare and provide Plans of Action and Milestones (POA&Ms) in support of risk mitigation efforts.
- Work closely with Configuration and Change Management (CCM), Business Continuity, Central Design Agency (CDA) and hosting and IA teams to coordinate and document changes that affect STIG documentation packages.
- Manage scans for server environments using established government approved and provided scanning solutions (scanning servers, running reports, analyzing results, and working with technical staff to resolve negative findings).

EOS PWS V2

Objective:

A. Implement and coordinate STIG compliance business processes.
B. Prepare and coordinate the efforts associated with STIG compliance determinations in support of applications and hosting environments.
C. Ensure STIG compliance is maintained and documented.
D. Manage server scans.

Deliverables

0018 - STIG Compliance Documentation
0019 - Security Scan Results and Actions stored in central repository

EOS PWS V2

3.4 Continuous Process Improvement and Quality Assurance

3.4.1 Data and Document Management

Overview: The Independent Verification and Validation (IV&V) team, within NITC's Enterprise Operations Division, provides document management, change management, configuration management, quality assurance services.

Work Description: The Contractor shall perform the following tasks:

- Develop and manage policies and procedures for Total Record and Information Management (TRIM) and NAVFAC Enterprise Library.
- Develop, implement, and sustain data and document management SOPs.
- Plan and execute complex assignments and develop new methods, approaches and procedures.
- Convert existing business process documents into the NAVFAC Business Management System (BMS) format and publish to the BMS.
- Determine the merits of proposed data and document management systems.
- Evaluate and recommend new or enhanced data and document management services.
- Design, customize, maintain, and support websites and web pages. For IV&V requirements.
- Develop, revise, and maintain desktop guides for configuration management, change management, portfolio management and quality assurance.

Objective:

A. Develop, implement and maintain process flows..
B. Develop, implement and maintain procedures.
C. Develop, implement and maintain policy.
D. Develop, implement and maintain desktop guide
E. Develop and present metric reports.

Deliverables

0020 - Document Management Process Flow
0021 - Document Management Procedure
0022 - Document Management Policy
0023 - Document Management Desktop Guide
0024 - Document Management Metric Reports

3.4.2 Change Management

Overview: Change management involves managing and providing oversight for all approved, documented, tracked, reported, and verified change action.

Work Description: The Contractor shall perform the following tasks:

- Provide oversight to verify changes are approved, documented, tracked, and reported.

EOS PWS V2

- Coordinate and manage change management and operations control board meetings.
- Coordinate and manage daily (weekday and weekend) change management activities.
- Manage the development, implementation, and sustainment of any automated change management systems.
- Develop and maintain procedures for submitting planned promotion and maintenance events for IA review prior to accepting event confirmation notices.
- Develop and maintain procedures for submitting planned promotion and maintenance events for Performance Monitoring Team review.
- Manage annual End of the Year and Beginning of the Year change management events.
- Manage submission and publishing calendar year planned promotion and maintenance events.
- Develop and present change management metric reports and data calls.

Objective:

A. Develop, implement and maintain process flows..
B. Develop, implement and maintain procedures.
C. Develop, implement and maintain policy.
D. Develop, implement and maintain desktop guide
E. Develop and present metric reports.

Deliverables

0025 - Change Management Process Flow
0026 - Change Management Procedure
0027 - Change Management Policy
0028 - Change Management Desktop Guide
0029 - Change Management Metric Reports

3.4.3 Configuration Management (CfM)

Overview: Configuration management involves managing and providing oversight for all hardware and software installations, functional changes, upgrades, sustainment, and disposals.

Work Description: The Contractor shall perform the following tasks:

- Provide oversight for NITC configuration management.
- Develop and maintain CfM plans and guides in support of hardware and software installations, functional changes, upgrades, sustainment, and disposals.
- Manage the development, implementation, and sustainment of a configuration management database.
- Coordinate and manage daily (weekday and weekend) configuration management activities.
- Develop policies and procedures for business systems' software, hardware, and device configuration baselines.
- Develop and maintain Microsoft Visio diagrams for business systems' software, hardware, and device configurations.
- Develop CfM closeout process flow, procedure and policy for Central Design Activity (CDA) and NAVFAC Application Service Provider (N ASP) events.
- Develop and present CfM metric reports and data calls.

Objective:

A. Develop, implement and maintain process flows..
B. Develop, implement and maintain procedures.

EOS PWS V2

C. Develop, implement and maintain policy.
D. Develop, implement and maintain desktop guide
E. Develop and present metric reports.
F. Develop and maintain configuration diagrams for each Business System.

Deliverables
0030 - Configuration Management Process Flow
0031 - Configuration Management Procedure
0032 - Configuration Management Policy
0033 - Configuration Management Desktop Guide
0034 - Configuration Management Metric Reports
0035 - Configuration Management Diagrams for each systems

3.4.4 Quality Assurance

Overview: Quality Assurance is responsible for providing verification, validation, audits, and reporting services.

Work Description: The Contractor shall perform the following tasks:

- Provide verification, validation, audit and reporting services.
- Develop, implement, and sustain quality assurance SOPs.
- Develop, implement, and sustain automated and manual IT systems' availability, functional and performance plans and test scripts.
- Prepare metric reports for IT systems' availability, functional, optimization, performance and personnel work performance.
- Consult with customers to develop and refine quality assurance requirements.
- Evaluate the feasibility of proposed new IT quality assurance projects.
- Evaluate and recommend adoption of new approaches to IT quality assurance services.
- Plan and execute complex, ad hoc quality assurance assignment and develop new methods, approaches, and procedures.

Objective:
A. Develop, implement and maintain process flows..
B. Develop, implement and maintain procedures.
C. Develop, implement and maintain policy.
D. Develop, implement and maintain desktop guide
E. Develop and present metric reports.

Deliverables
0036 - Quality Assurance Process Flows
0037 - Quality Assurance Procedures
0038 - Quality Assurance Policys
0039 - Quality Assurance Desktop Guide
0040 - Quality Assurance Metric Reports

FOR TWS V2

3.4.5 Portfolio Management

Overview: Portfolio Management is the centralized management of the portfolio of projects. This includes identifying, prioritizing, authorizing, managing, and controlling projects, programs, and other related work to achieve specific strategic business objectives.

The DON CIO has implemented business processes to ensure that Navy IT assets are efficiently managed and aligned with the warfighter priorities. The Navy has established Functional Area Managers (FAM) to execute the responsibility of directing migration, consolidation or retirement of applications and databases. The Department of the Navy Application and Database Management System (DADMS) is the authoritative data source for DON application and database portfolio management. The tool for managing the NAVFAC portfolio is the NAVAFAC Information Technology Enterprise Portal (NITEP).

Work Description: The Contractor shall perform the following tasks:

- Maintain application portfolio inventory utilizing Navy and NAVFAC tools (DADMS, NITEP, and ISF Tools). The NAVFAC Portfolio Team must administer NAVFAC data in three databases, keeping information aligned in each for approximately 350 active applications or systems.
- Support application portfolio management implementation policy using Navy and NAVFAC guidance and direction and Navy FAM policy including implementing Logistics FAM's Portfolio Manager Concept of Operation.
- Perform analysis, demonstrations, and lead briefings to market and promote portfolio initiatives. Represent NAVFAC in a variety of meetings with other Navy and DoD organizations. Assist in collecting, tracking, and updating metric information and brief preparation.
- Perform portfolio change management involving research and abbreviated business case analyses for IT investment requests using templates to determine if request supports the portfolio. The support includes aiding those with the portfolio subsections delegated to the responsible business and support owners.
- Assist in data collection and tracking of individual application testing and certification. Coordinate rationalization, approval, and testing of business applications.
- Provide support to answer questions and service requests. Requests for information and assistance come from subordinate activities, FAMs, Umbrella managers, and other Navy command organizations. Duties require a great deal of flexibility and coordination with the virtual team members.
- Develop and maintain portfolio management SOPs for new acquisition, upgrade, sustainment, decommission, and disposal of software and hardware.
- Develop and maintain process flow, baselines, procedures, and policies for management of software media, downloaded software, and software source code and configuration files.
- Manage and monitor software licensing, including initial purchase and upgrades, and report on technical support contract expirations and end of lifecycle dates.
- Develop and maintain process flow, baselines, procedures, and policies for management of servers, storage, and network devices.
- Monitor and report hardware maintenance contract expirations and end of lifecycle dates.
- Develop and present portfolio management metric reports and data calls.

Objective:

A. Develop, implement and maintain process flows..
B. Develop, implement and maintain procedures.
C. Develop, implement and maintain policy.
D. Develop, implement and maintain desktop guide
E. Develop and present metric reports.

FOUO PWS V2

F. Develop and maintain software media baselines.
G. Develop and maintain software license baselines.
H. Develop and maintain server baselines.
I. Develop and maintain network device baselines.

Deliverables
0041 - Portfolio Management process flows
0042 - Portfolio Management procedures
0043 - Portfolio Management policys
0044 - Portfolio Management desktop guide
0045 - Portfolio Management metric reports
0046 - Software Media baselines
0047 - Software License baselines
0048 - Server baselines
0049 - Network Device baselines

3.4.6 Information Technology Infrastructure Library (ITIL)

Overview: NITC has developed a roadmap for adopting the Information ITIL framework. NITC requires support and services to help guide the organization in implementing and developing new ITIL processes and functions.

Work Description: The Contractor shall perform the following tasks:

- Manage the Information Technology Infrastructure Library:
- Serve as the ITIL subject matter expert to the organization.
- Provide expert guidance to process owners in developing and maintaining each specific process area.
- Coordinate between process owners to ensure interdependencies align with the ITIL framework.
- Facilitate process development meetings, provide informal ITIL awareness sessions, and give feedback assistance in the development of ITIL processes.
- Provide guidance on metric tracking and reporting.
- Generate and present progress reports.
- Conduct awareness training sessions to improve knowledge of the ITIL framework, give general advice on adopting the framework, provide references for additional research and give general feedback on existing efforts.

Objective
A. Develop, implement and sustain standard operating procedures.
B. Develop, implement and sustain desktop guides.
C. Develop and maintain hardware and software baselines.
D. Develop and present metric reports

EOS PWS V2

3.5 End-to-End (E2E) Performance Management Support

3.5.1 End-to-End Performance Management

Overview: End-to-End performance management is essential to optimizing the utilization of NAVFAC's system resources. Proper management involves measuring current capabilities, recognizing trends, and making appropriate adjustments to satisfy user and management requirements.

This task involves analytical, technical, system administration and management support for the planning, implementation, documentation and administration of the Network End-to-End Performance Management function.

Work Description: The Contractor shall perform the following tasks:

- Support network E2E management using Navy and NAVFAC guidance and direction.
- Perform research and analysis to formulate specific application response time targets along with validated industry benchmark comparisons. This includes analyzing and interpreting measurements and metrics collected and rendered by the government's monitoring toolset, the Hewlett-Packard Business Technology Optimization suite.
- Provide technical and administrative support for network and application service provider monitoring tools. This includes performing upgrades of current software environment to latest approved versions with follow on tuning to ensure optimal performance. Upgrades should be performed with minimal downtime and with assured historical data retention.
- Implement basic and advanced application and business process monitoring templates as appropriate.
- Research and establish notification alerts for monitored applications to notify NITC OPSWATCH, NITC Technical support personnel, and NMCI support and operations personnel of the need for inspection and possible corrective action on system measurement and optimization components.
- Utilize data provided by the government's monitoring toolset, the Hewlett-Packard Business Technology Optimization suite, to develop reports regarding system availability and performance of monitored NAVFAC business applications.
- Provide support to answer questions and service requests for information. Such requests come from subordinate NAVFAC activities as well as other Navy command organizations.
- Assist in collecting, tracking, updating and rendering metrics information regarding availability and E2E performance of business applications. Using current BPM scripts and BPM data, develop Business Availability Center (BAC) views and reports for system availability and performance of hosted business systems.
- Perform analysis, demonstrations, and lead briefings to market and promote network E2E initiatives. This includes representing NAVFAC in a variety of meetings with other Navy and DoD organizations.

Objective

EOS PWS V2

3.6 Project Management

3.6.1 Project Management and Planning

Overview: Throughout the life of this task order, project management support is needed to ensure the successful and timely completion of all tasks and deliverables.

The schedules for this task order will be maintained and stored electronically in the government provided solution.

Work Description: The Contractor shall perform the following tasks:

- Create, maintain, and submit a weekly Microsoft Project schedule to the Government on all projects, using work breakdown structure. The schedule will include a report that provides a status at an agreed upon task level, noteworthy accomplishments, and challenges that need attention.
- Create and maintain an Execution Plan (EP) based on the input from the CDA, NASP, Operations, development team, and user community upon receipt of a work request. The EP will be broken out in a manner that facilitates tracking of the various Microsoft Project components and shall include near term (current six-month period), medium-term (six to 12 months), and long-term (one to three years) objective and timelines. The EP shall include functional and technical objectives.

Objective
A. Create and maintain a Microsoft Project Schedule and Execution Plan.

Deliverable
0054 - POA&M

3.6.2 Status Reports and Meetings

Overview: The Contractor shall provide, on an ongoing basis, project management information via status reports and/or meetings.
All meetings and reviews shall be held either at the Ordering Officer, the Contractor's office, or at any other location as specified by the Ordering Officer within the geographic locations identified in the task order.

Work Description: The Contractor shall perform the following tasks:

- Participate in monthly Task Review meetings with the Government Application Project Lead to discuss the required Monthly Financial Summary Report and Monthly Summary Report.
- Provide a comprehensive status briefing of this task order to the NAVFAC CIO, NITC management, and other parties at a minimum of four (4) times per year. Draft presentations shall be provided to the Government ten (10) business days prior to the start of the meeting. The Government will review and provide comments within five (5) business days after receipt of draft presentation. Final presentations shall be posted to the NAVFAC Portal in the appropriate location one (1) business day prior to the start of the meeting.
- Provide analytical and technical support to various Configuration Control Boards (CCBs) that support each major functional area or Information System. The Contractor shall attend the CCBs and collect discussion data points and action items and provide written documentation covering these discussions to the Task Order Manager (TOM) five (5)

EOS PWS V2

business days after each meeting. The Contractor shall also be required to give presentations at the CCB meetings and to lead discussions.

Objective
A. Provide burn rate chart to government.
B. Attend scheduled Task Review Meetings.
C. Provide draft and final meeting materials and presentation.

Deliverable
0055 - Bi-weekly Budget and Burn Rate Report
0056 - Monthly Financial Report

3.6.3 Program Oversight

Overview: Program and contract management requires day-to-day oversight of contracts and performs tasks such as reviewing and approving deliverables and invoices.

Work Description: The Contractor shall perform the following tasks:

- Generate, maintain, and submit electronic, bi-weekly charts that provide information on current and projected cumulative costs, labor hours, expended and projected percentage of work accomplished, and other metrics plotted against time. The Contractor shall include supporting detail information in spreadsheet format.
- Submit to Government inspections upon receipt of deliverables. In the absence of a formal agreement, the Government will complete the review of draft deliverables within five (5) business days of receipt and will complete the review and acceptance (or rejection) of final deliverables within 10 business days of receipt.
- Provide monthly cost and execution reports. Cost reports at the task level must be provided in spreadsheet format.

Objective
A. Provide accurate and timely monthy invoices to the government on.

Deliverable
0057 - Month Invoice

EOS PWS V2

3.7 Performance Requirements Summary Matrix

Item	Performance Objective	Performance Standard and Acceptable Quality Level (AQL)	Methods of Performance Assessment
3.1.1 Incident Management Support			
3.1.1.A	Provide courteous, efficient and timely responses to all customers.	The ratio of Operations Watch customer service complaints to the total tickets handled cannot exceed 3%.	Government review of tickets along with feedback from users.
3.1.1.B	Receive, analyze, resolve, escalate, and coordinate the resolution of user issues	Issues defined as incidents will be reviewed by a government representative for timely responses, and adherence to documented ticket management practices. Outstanding incidents that have not been resolved within a reasonable amount of time will be the prime candidates for review.	Government review of tickets, feedback from NITC application managers and NAVFAC users.
3.1.1.C	Document user and facility issues in the tracking system.	No less than 95% of all incident reports reviewed should contain complete detailed information about customer contact information, end-user symptoms, end-user account information (if applicable), and application info (if applicable).	Government review of trouble tickets.
3.1.1.D	Provide metrics relating to the quantity, category, status and resolution of issues.	Information accurately reflects the status of issues and is provided in accordance with agreed upon formats and timeframes.	Government review.
3.1.2 Process Monitoring Support			
3.1.2.A	Insure issues are acknowledged, logged, and acted on in a timely manner, as defined by the procedures set forth for each monitoring system.	Issues are acknowledged and acted on in a timely manner, as defined by the procedures set forth for each monitoring system.	Government review of trouble tickets and management feedback.

EOS PWS v2

3.1.2.B	Review and maintain NITC Operations Watch procedures	In conjunction with a designated government representative, Operations Watch will review, update, and maintain external (*clarify procedure covered*) procedures on a quarterly basis. As proof of acceptable quality, both the Operations Watch lead and the government representative will formally acknowledge or sign for the successful completion of a procedure review or update.	Random review of team procedures and feedback from NITC application managers and NAVFAC users.
3.1.3 Event/Incident Notification Support			
3.1.3.A	Document operational status, application and facility issues and share information as required to NAVFAC users and management	In conjunction with designated government representative, Operations Watch will review, update and maintain procedures on a consistent and regular basis.	Government review by IV&V event coordinator for possible anomalies.
3.1.3.B	Provide reports and metrics to NAVFAC management regarding operational status and support issues.	Information shall accurately reflect the status of issues and be provided in accordance with agreed upon formats and timeframes	Government review of IV&V event feedback and possible anomalies.
3.1.3.C	Communicate and coordinate with NAVFAC CIO Help Desks across NAVFAC organizations worldwide and provide standard operating procedures and policies for use by the NAVFAC Help Desk community	In conjunction with a designated government representative, review, update and maintain procedures on a quarterly basis.	Government review.
3.1.4 Inventory and Asset Control Support			
3.1.4.A	Provide video conferencing support arrangements via ticketing system process and direct audio conferencing support.	Video conferencing support and requests will be tacked using the support ticketing system (STS).	Government Review
3.1.4.B	All data center hardware and assets are secured and accounted for in the DPAS.	All assets in DPAS should be accounted for in periodic physical inventory and reporting.	Government Review
3.1.4.C	Destruction and removal of equipment shall be done in accordance with federal, state, local and DoD guidance.	All assets removed and destroyed should be updated in DPAS and records should be managed based on DOD guidelines. Periodic reports should be produced.	Government Review
3.1.4.D	Maintain and update processes and procedures for managing inventory.	All processes and procedures should be reviewed periodically and maintained in a central location.	Government Review

RFS PWS V2

3.1.4.E	Staff must have access to DPAS system	Training and Account required.	Government Review
3.1.5 Facility Management and Physical Security Support			
3.1.5.A	Provide support in maintaining building entry system, security alarms, surveillance equipment and monitoring.	Defending against unauthorized access to facility and its assets, systems, networks, and data. Eliminate or minimize issues relating to the facility and its equipment.	Government Review
3.1.5.B	Provide support in developing and granting appropriate entry to NITC facility and access to assets including hardware and software.	Assist in defending against unauthorized access to the facility and its assets, systems, networks, and data. Perform walk-through and checks for such things as jarred doors and open windows after normal business hours.	Government Review
3.1.6 Office and Reception Duties			
3.1.6.A	Greet visitors and provide directions and guidance to various locations in the facility and provide information about the facility and personnel to authorized guests	Calls and visitors should be directed to requested locations and personnel.	Government Review
3.1.6.B	Insure visitors are easily identifiable.	Visitors should be identified, assigned visitor badges, and logged (Data Center)	Government Review
3.2 Local Operations Support and Help Desk			
3.2.A	Provide operations support.	Operational tasks are completed on time.	Government review.
3.2.B	Provide S&T seat configuration management.	Systems are reliable, compatible and interoperable. 98% of tasks are completed within 3 business days.	Government review.
3.2.C	Insure calls are answered promptly by operations/help desk personnel.	Calls are answered within 30 seconds or a voice mail can be left. Calls shall be returned within 1 hour of receipt.	Government review of operations along with feedback from users.
3.2.D	Time to resolve user problems or answer question is as short as possible.	95% of calls received are resolved within 1 business day.	Government review of call activity logs.
3.2.E	Operations/help desk personnel are courteous and efficient.	No more than 2 complaints are received per month regarding courtesy and/or lost/late messages. All e-mails and voice mails are responded.	Government review of trouble tickets along with feedback from users.
3.2.F	Maintain operations/help desk documentation.	Documentation is current and accurate.	Government review.
3.2.1 Navy Marine Corps Intranet (NMCI) Continuity of Service Contract (COSC) Support			

EOS PWS V2

3.2.1.A	Support and monitor MACs at an enterprise level.	All requests received will be acknowledged within 4 working hours. Status/updates will be logged within 3 business days of receipt. No more than 2 valid complaints about the service per month. No more than 10% logged late.	Customer feedback. Government review of status/updates.
3.2.1.B	Provide MAC projections for current and out year requirements.	Monthly report submitted no later than 6 business days after the end of a month. No more than 15% reports received late.	Government review.
3.2.1.C	Setup and maintain new service request management groups.	All requests acknowledged within 4 working hours. Updates will be posted within 1 business day of notification of completion. No more than 2 complaints in a month. No more than 10% of updates posted late.	Government review.
3.2.2 Cyber Asset Reduction and Security (CARS) Support			
3.2.2.A	Migration solutions identified.	Conduct scheduled bi-weekly meeting with each NAVFAC COSC/ONE-NET transitioning activity to refine and track CARS Case execution plan solutions, or identify new, alternate, or backup solutions for functionality migration. Bi-weekly meetings documented within 5 business days. Issue papers with recommended migration solution developed within 10 business days	Periodic (weekly/bi-weekly) CARS teleconferences with NAVFAC CARS POC, and review of monthly CARS issues/execution status reports for NAVFAC enterprise and individual NAVFAC activities.
3.3.1 Information Assurance Certification and Accreditation (C&A) Support			
3.3.1.A	Implement and coordinate IA C&A business processes.	Attendance required at related meetings and collaboration with CDA/NASP to ensure timeliness. Efforts reported weekly.	Government Review
3.3.1.B	Prepare and coordinate the efforts associated with completing C&A documents in support of applications and hosting environments.	DIACAP requirements are completed within two days of requirement approval with less than 10% rework.	Government Review
3.3.1.C	Ensure C&A documents are updated as changes are implemented.	Packages updates are coordinated with system owners/liaisons and completed within 30 days of any change.	Government Review
3.3.2 Information Assurance Compliance and Audit Support			
3.3.2.A	Implement and coordinate IA compliance business processes.	Compliance Status reports submitted for review within one day of agreed upon completion with less than 10% rework.	Government review

EOS PWS V2

3.3.2.B	Prepare and coordinate the efforts associated with IA compliance determinations for all business systems.	Attendance required at related meetings and collaboration with the NASP to ensure compliance. Efforts reported weekly.	Government review
3.3.2.C	Ensure IA compliance is maintained and documented.	Manages master compliance documents and DIACAP POA&M and individual Information System POA&Ms.	Government review
3.3.2.D	Manage server scan results and vulnerabilities.	Ensures 100% of required scans, SRRs, and checklists are completed on a timely basis and stores electronically.	Government review
3.3.2.E	Perform periodic IA compliance auditing, ensuring results are documented and reported within two (2) business days.	Compliance Status and audit result reports submitted for review within two business days of agreed upon completion. Efforts reported quarterly.	Government review
3.3.3 Information Assurance Continuity and Recovery Planning Support			
3.3.3.A	Develop and maintain Business Recovery processes documentation.	Master Continuity, Contingency, and Recovery processes, including Alternate-Site recovery documents, are accurate and complete. Submitted for review within two days of agreed upon completion with less than 10% rework.	Government Review
3.3.3.B	Manage project efforts for full implementation of an Alternate Site facility in collaboration with the NASP technical project manager.	Attendance required at related meetings and collaboration to ensure compliance. Coordinates efforts and ensures project stays on track through frequent correspondence with all involved parties. Efforts reported weekly.	Government Review
3.3.3.C	Develop and maintain processes related to Recovery execution.	Ensure all NITC hosted applications are maintain compliance with reporting dates and contain accurate and up-to-date recovery procedures.	Government Review
3.3.3.D	Perform annual Contingency and Incident Reponses (CIR) tests and report results.	Lead annual contingency testing and provide documentation compliant with DIACAP process requirements.	Government Review
3.3.3.E	Provide business Recovery solution recommendations.	Studies, recommendations and reports are accurate, complete, and provided as requested 100% of the time for government review.	Government Review
3.3.4 Information Assurance Certification and Accreditation Technical Writing Support			
3.3.4.A	Provide technical writing support for NAVFAC IA and C&A documentation.	Contractor provides technical documents to the Government five calendar days prior to final document due dates as assigned for review and approval, with less than 10% rework. Once approved, final documents will be provided in electronic format.	Government Review
3.3.4.B	Develop weekly IA status reports to track IA and C&A metrics.	Provide metric-based reports including project statuses and timelines weekly.	Government Review

EOS PWS V2

3.3.5 Information Assurance Security Technical Implementation Guide (STIG)			
3.3.5.A	Implement and coordinate STIG compliance business processes.	Documentation is accurate, complete and provided on time.	Government review and feedback.
3.3.5.B	Prepare and coordinate the efforts associated with STIG compliance determinations in support of applications and hosting environments.	Documentation is accurate, complete and provided on time.	Government review.
3.3.5.C	Ensure STIG compliance is maintained and documented.	STIGs are implemented or mitigation plans developed.	Government review.
3.3.5.D	Manage server scans.	Server scans are completed and results published on time.	Government review.
3.4.1 Data and Document Management			
3.4.1.A	Develop, implement and maintain process flows.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.1.B	Develop, implement and maintain procedures.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.1.C	Develop, implement and maintain policy.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.1.D	Develop, implement and maintain desktop guide.	Draft Versions submitted for review 1 month after request. Final Versions for review 1 month after draft is approved.	Government Review.
3.4.1.E	Develop and present metric reports.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved.	Government Review.
3.4.2 Change Management			
3.4.2.A	Develop, implement and maintain process flows.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.2.B	Develop, implement and maintain procedures.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.2.C	Develop, implement and maintain policy.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.2.D	Develop, implement and maintain desktop guide.	Draft Versions submitted for review 1 month after request. Final Versions for review 1 month after draft is approved.	Government Review.
3.4.2.E	Develop and present metric reports.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved.	Government Review.
3.4.3 Configuration Management (CfM)			
3.4.3.A	Develop, implement and maintain process flows.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.

EOS PWS V2

3.4.3.B	Develop, implement and maintain procedures.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.3.C	Develop, implement and maintain policy.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.3.D	Develop, implement and maintain desktop guide.	Draft Versions submitted for review 1 month after request. Final Versions for review 1 month after draft is approved.	Government Review.
3.4.3.E	Develop and present metric reports.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved.	Government Review.
3.4.3.F	Develop and maintain configuration diagrams for each Business System.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved. The 35-40 final version of diagrams should be complete in 70-80 weeks.	Government Review.
3.4.4 Quality Assurance			
3.4.4.A	Develop, implement and maintain process flows.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.4.B	Develop, implement and maintain procedures.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.4.C	Develop, implement and maintain policy.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.4.D	Develop, implement and maintain desktop guide.	Draft Versions submitted for review 1 month after request. Final Versions for review 1 month after draft is approved.	Government Review.
3.4.4.E	Develop and present metric reports.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved.	Government Review.
3.4.4 Portfolio Management			
	Develop, implement and maintain process flows.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
	Develop, implement and maintain procedures.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
	Develop, implement and maintain policy.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
	Develop, implement and maintain desktop guide.	Draft Versions submitted for review 1 month after request. Final Versions for review 1 month after draft is approved.	Government Review.
	Develop and present metric reports.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved.	Government Review.
	Develop and maintain software media baselines.	Baseline should be completed 3-4 weeks after request. Baselines should be updated and submitted for QA review bi-weekly.	Government Review.

EOS PWS V2

	Develop and maintain software license baselines.	Baseline should be completed 3-4 weeks after request. Baselines should be updated and submitted for QA review bi-weekly.	Government Review.
	Develop and maintain server baselines.	Baseline should be completed 3-4 weeks after request. Baselines should be updated and submitted for QA review bi-weekly.	Government Review.
	Develop and maintain network device baselines.	Baseline should be completed 3-4 weeks after request. Baselines should be updated and submitted for QA review bi-weekly.	Government Review.
3.4.4 Information Technology Infrastructure Library (ITIL)			
3.4.4.A	Develop and present configuration management project plans and requirements documents.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.4.B	Develop and present change management project plans and requirements documents.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.4.C	Develop and present release management project plans and requirements documents.	Draft Versions submitted for review 2 weeks after request. Final Versions for review 2 weeks after draft is approved.	Government Review.
3.4.4.D	Develop and present ITIL based metric reports.	Draft Versions submitted for review 1 week after request. Final Versions for review 1 week draft is approved.	Government Review.
3.5.1 End-to-End Performance Management			
3.6.1 Project Management and Planning			
3.6.1.A	Create and maintain a Microsoft Project Schedule and Execution Plan.	Provide POA&M to Work Requestor 2 days prior to schedule project review dates.	Government Review
3.6.2 Status Reports and Meetings			
3.6.2.A	Provide burn rate chart to government	Provide monthly burn rates charts to government.	Government receives accurate reports on time.
3.6.2.B	Attend scheduled Task Review Meetings.	Contractor provides draft presentations to the Government 5 calendar days prior to the start of the meeting. Final presentations shall be due in electronic format, 2 calendar days prior to the start of the meeting.	Government review and acceptance of contractor provided draft and final copies of meeting materials and presentations.

EOS PWS V2

3.6.2.C	Provide draft and final meeting materials and presentation.	Facilitate monthly and quarterly Contract Status reviews with government representatives. Prepares and perform PowerPoint presentation during monthly and quarterly Contract Status Reviews.	Government review and acceptance of contractor provided draft and final copies of meeting materials and presentations.
3.6.3 Program Oversight			
3.6.3.A	Provide accurate and timelymonthy invoices to the government on.	Monthly Invoices are timely and accurate	Government review

EOS PWS V2

3.8 Deliverables

Item	Deliverable	Format	Date Required
3.1.1	A001 - User Issues Metrics		
3.1.2	0002 - Up-to-date NITC Operations Watch Procedure		
3.1.3	0003 - OperationS status report		
3.1.4	0004 - Up-to-date asset inventory in DPAS		
3.1.5			
3.1.6	0005 - Completed Visitors Log		
3.2	0006 - Up-to-date Operations & HelpDesk procedures		
3.2.1	0007 - MAC List (current and projected)		
3.3.1	0008 - Fully maintained C&A documents		
3.3.1	0009 - Up-to-date IA C&A business processes		
3.3.2	0010 - Up-to-date IA compliance business processes		
3.3.2	0011 - IA Compliance Audit Reports		
3.3.2	0012 - IA Scan Results and Vulnerabilities Reports		
3.3.3	0013 - Business Recovery Process Document		
3.3.3	0014 - Business Recovery Testing Plan		
3.3.3	0015 - Annual Contingency and Incident Reponses (CIR) Test Reports		
3.3.4	0016 - Completed IA and C&A Packages		
3.3.4	0017 - Weekly IA & C&A Tracking Reports		
3.3.5	0018 - STIG Compliance Documentation		
3.3.5	0019 - Security Scan Results and Actions stored in central repository		
3.4.1	0020 - Document Management Process Flow		
3.4.1	0021 - Document Management Procedure		
3.4.1	0022 - Document Management Policy		
3.4.1	0023 - Document Management Desktop Guide		
3.4.1	0024 - Document Management Metric Reports		
3.4.2	0025 - Change Management Process Flow		
3.4.2	0026 - Change Management Procedure		
3.4.2	0027 - Change Management Policy		
3.4.2	0028 - Change Management Desktop Guide		
3.4.2	0029 - Change Management Metric Reports		
3.4.3	0030 - Configuration Management Process Flow		
3.4.3	0031 - Configuration Management Procedure		
3.4.3	0032 - Configuration Management Policy		
3.4.3	0033 - Configuration Management Desktop Guide		
3.4.3	0034 - Configuration Management Metric Reports		
3.4.3	0035 - Configuration Management Diagrams for each systems		
3.4.4	0036 - Quality Assurance Process Flows		
3.4.4	0037 - Quality Assurance Procedures		
3.4.4	0038 - Quality Assurance Policys		
3.4.4	0039 - Quality Assurance Desktop Guide		
3.4.4	0040 - Quality Assurance Metric Reports		
3.4.5	0041 - Portfolio Management process flows		

PWS V2

3.4.5	0042 - Portfolio Management procedures		
3.4.5	0043 - Portfolio Management policys		
3.4.5	0044 - Portfolio Management desktop guide		
3.4.5	0045 - Portfolio Management metric reports		
3.4.5	0046 - Software Media baselines		
3.4.5	0047 - Software License baselines		
3.4.5	0048 - Server baselines		
3.4.5	0049 - Network Device baselines		
3.4.6	0050 - Configuration Management Project Plan and Requirements Documents		
3.4.6	0051 - Change Management Project Plan and Requirements Documents		
3.4.6	0052 - Release Management Project Plan and Requirements Documents		
3.4.6	0053 - ITIL Based Metric Reporting Template		
3.6.1	0054 - POA&M	MS Project	As Needed
3.6.2	0055 - Bi-Weekly Budget and Burn Rate Report	Powerpoint	Bi-Weekly
3.6.2	0056 - Monthly Financial Report	Powerpoint	Monthly
3.6.3	0057 - Monthly Invoice		Monthly

EOS PWS V2

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

Information:
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 task order.

Equipment and Facilities:
The Government will furnish the necessary facility requirements to maintain an office environment, including a workspace, furnishings, fax and telephone services, document reproduction capabilities, and other items necessary to maintain an office environment.

The Government will provide the required number of software licenses necessary to accomplish this task order 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 NAVFAC Information Systems to accomplish assigned work covered in this task order when support effort is not required to be on-site in government spaces.

The Government will provide hand held equipment, as required, to accomplish assigned work covered by this task order.

EOS PWS V2

Utilities:
All utilities in NAVFAC facilities will be available for the Contractor's use in performance of duties as outlined in this PWS. The Contractor shall instruct employees in utilities conservation practices. The contractor shall be responsible for operating under conditions that preclude the waste of utilities.
Access:
The Government shall provide necessary computer resources required to perform assigned tasks, including NMCI workstations, access to terminals, printers, software, data, network resources, etc.

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

6. Contractor Furnished Information, Services, And Equipment

The Contractor shall provide technical support as needed to meet the requirements of the task order 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.

Compliance with current and future DoD, DON, CYBERCOM, NNWC, NMCI, NAVFAC, and local guidance and directives is required for all Contractor workstations connecting remotely to NAVFAC networks or Information Systems.

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, but will generally conform to the NAVFAC business core-hours of 0600-1800. Certain tasks may require work and travel after normal business hours, including evenings, weekends, and holidays.

Actual hours of work will be agreed upon task order start up.

7.2 Period of Performance:

This task order 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 the task order 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 task order, including the exercise of any options under this clause, shall not exceed three (3) years.

EOS PWS V2

7.3 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 task order.

Travel arrangements and costs shall be in accordance with the Joint Federal Travel Regulations. Before undertaking any travel in performance of this task order, the Contractor shall have the travel approved, in writing, by the TOM or Navy Technical Representative (NTR). In an urgent situation, telephonic/verbal approval by the TOM or NTR is acceptable, with the understanding that the written approval request shall be provided within ten (10) calendar days. Any travel expenses that are invoiced to the government shall be accompanied with backup or supporting documents

7.3.1 Air Travel:

To the maximum extent practical, the Contractor shall 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.

7.3.2 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.

7.4 Training:

The Government will not allow costs, nor reimburse costs, associated with the Contractor training employees in an effort to attain and/or maintain the minimum personnel qualification requirement(s), nor any specialized certification requirements of this task order.

The following are considered training for the purposes of this clause:

- Workshop, Conference, or Symposium attendance,
- IA Workforce certification training, exams, and maintenance events;
- Any event intended to procure Continuous Learning (CL) points for certification maintenance.

Contractor attendance at workshops, conferences, or symposiums, and all IA Workforce certification training and exams are considered training for purposes of this clause.

7.5 Monthly Status Reports:

The contractor shall submit a monthly status report consisting of an Executive Summary detailing the major accomplishments, activities, burn rates, and financial status of the previous month. These reports shall contain an accurate and timely summary account of major accomplishments, activities, actual and projected burn rates (hours and funds), and the financial status of the contract.

Reports will be provided to the Work Requestor in Adobe PDF format. Alternate report formatting may be considered at the discretion of the Work Requestor.

EOS PWS V2

The Contractor shall submit monthly reports via E-Mail to the Work Requestor no later than five (5) business days from the first day of the following month.

7.6 Contractor Identification

All Contractor staff shall ensure, to the greatest extent possible, that 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.

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.

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.

7.7 Intellectual Property:

This task order is funded by the United States Government.

All intellectual property generated and/or delivered pursuant to this task order shall be subject to appropriate federal acquisition regulations, which entitle the Government to the following:

- 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 task order, and,
- A nonexclusive and irrevocable worldwide license to reproduce all works, including technical and scientific articles, produced during this task order.

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

7.8 Transition between Contract and Continuity of Service:

EOS PWS V2

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

The Contractor must recognize that services under this task order are vital to the Government and must be continued without interruption and that upon task order 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 Contractor shall not recruit on Government property or otherwise act to disrupt Government business. Within ten (10) calendar days of a task order award, the Contractor shall inform the appropriate TOM of incumbent personnel, who will not be placed on the task order.

The Contractor shall have management and administrative support in place to fulfill work requirements at time of commencement of the task order 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 task order. Appropriate task order management personnel shall meet with the successor Contractor to coordinate task order transition. Discussions shall include personnel transition to the successor Contractor, and the transition of task order 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.

EOS PWS V2

Appendices

Appendix A - **References and Publications**

(a) DoDI 8510.01, *DoD Information Assurance Certification and Accreditation Process (DIACAP)*, 28 November 2007

(b) *Department of the Navy DoD Information Assurance Certification and Accreditation (DIACAP) Handbook* 15 July 2008

(c) *C&A Guidance for Automated C&A Scanning and Configuration Tools*, 27 July 2009

(d) Naval Telecommunication Directive 08-08, *Network Topology Diagram Requirements*, August 2008

(e) Memo from Commander, Space and Naval Warfare Systems Command, *Qualification Standards and Registration Procedures for Navy Validators*, 18 March 2010

(f) NIST Special Publication 800-34 *Contingency Planning Guide for Information Technology Systems*, June 2002

(g) NIST Special Publication 800-61 *Computer Security Incident Handling Guide*, March 2008

(h) SECNAVINST 5239.2, *Information Assurance Workforce* Management, May 2009

(i) DTG R 181430Z MAY 09, *Department of the Navy Privacy Impact Assessment (PIA) Guidance*

(j) NAVFAC DIACAP Policy, 16 June 2010

(k) *New C&A Process Guide*, 8 July 2008

(l) DoDI 8500.2, *Information Assurance (IA) Implementation*, 06 February 2003

(m) DoDI 8570.01-M, *Information Assurance Workforce Improvement Program*, Change 1, 15 May 2008

(n) Subchapter III of Chapter 35 of title 44, United States Code, *Federal Information Security Management Act (FISMA) of 2002*

EOS PWS V2

Tables

Table 01 - Help Desk Support Services and IAT Level Requirements

Service and Support Tasks	
Operation Job Scheduling and Maintenance (Tier 1)	
Develop, maintain and revise existing operations schedules for daily and other regularly scheduled data transfers and update jobs. End user access only.	No cert required
Monitor job schedules and their execution status. End user access only.	No cert required
Operation Job Scheduling and Maintenance (Tier 2)	
Modify jobs for data transfer and updates. Privileged administration access required.	IAT1
VTC and Equipment Pool Support (Tier 2)	
Provide technical and operations support for the unclassified Defense Messaging System (DMS). End user access only.	No cert required
Provide assistance with the scheduling and set-up of Video Teleconferences (VTC) and Training rooms. Some requests may require coordination with the enterprise. Provide conference lines for attendees connecting via telephone.	No cert required
Manage, track and operate a loan pool of equipment for use by traveling employees or other offsite use.	No cert required
Help Desk/Service Desk Support (Tier 1)	
Assist end users with administrative requirements of associated S&T community of interest (COI), including assistance with forms, software configuration, licensing and inventory control.	No cert required
Provide general end-user and legacy application Help Desk support, including requests received via phone, email, walk-up, or submission by an automated trouble tracking tool. The help desk shall capture documentation of problems and solutions using NAVFAC software. End user access only.	No cert required
Track the resolution of user problems, keeping the user informed of progress. Follow-up with the user after problem resolution to ensure the solution was satisfactory and complete prior to closing the trouble call.	No cert required
Provide end-user liaison support for accessing network (NMCI) services.	No cert required
Manage distribution lists that are maintained on NMCI.	No cert required
Maintain the Field Help Desk Documentation. This documentation shall include technical manuals, trouble tracking tool, help desk knowledge base and standard Field Operations/Help Desk procedures. The Contractor shall submit changes for review and acceptance by the government.	No cert required
Provide technical and operations support for desktop applications such as the Microsoft Office products. Privileged administration access not required.	No cert required
Assist users in tasks that allow for a more efficient operation of their desktop system. Privileged administration access not required.	No cert required

EOS PWS V2

Help Desk / Service Desk Support (Tier 2)	
Provide technical and operations support for desktop applications such as the Microsoft Office products and assist users in tasks that allow for more efficient operation of their desktop systems. Privileged administration access required.	IAT1
Assist with the installation of government owned peripherals devices on NMCI workstations. Privileged administration access required.	IAT1
Provide end-user support, including configuration assistance, for various software applications used by the activity. Privileged administration access required to modify workstation configuration.	IAT1
Manage Kiosk machines. Coordinate software installation with end users, or install software for end users as required. Assist end users with administrative requirements of any required forms, software configuration, software licenses and inventory control. Privileged administration access required for software installation.	IAT1
Maintain / modify application databases using privileged administration access rights.	IAT1
Provide Office product application support, including access / excel databases, where privileged access rights are used to modify the configuration, macros or data files of Government owned applications or systems.	IAT1
Application support providing backup and restoration of system, database, or application on Government owned application, workstation, server or network	IAT1
Application Testing of Government owned applications and systems. End user access only.	
Application Testing of Government owned applications and systems. Privileged access required to modify application databases or develop and execute test scripts.	IAT1
S&T Seat Support (Tier 2)	
Provide an NMCI Science and Technology (S&T) configuration manager. The S&T CM is responsible for providing configuration support to the end-user for these workstations. Privileged administration access required to modify workstations configuration.	IAT1
Coordinate software installation with end users, or install software for end users as required. Privileged administration access required to modify workstation configuration or install software.	IAT1

EOS PWS V2

Attachments

Attachment 01 - Enterprise Business Systems

P L A C E H O L D E R

EOS PWS V2

Attachment 02 - Common Operating Environment (COE)

P L A C E H O L D E R

EOS PWS V2

Attachment 03 - Non Disclosure Form

P L A C E H O L D E R

EOS PWS V2

Attachment 04 - Department of Homeland Security Employment Eligibility Verification, Form I-9

P L A C E H O L D E R

EOS PWS V2

Attachment 05 - Contractor Verification System (CVS)

P L A C E H O L D E R

EOS PWS V2

Attachment 06 - System Authorization Access Request Form (SAAR)

P L A C E H O L D E R

EOS PWS V2