Performance Work Statement
Navy Enterprise Resource Planning (ERP) Program Management Office
- Information Assurance (IA) and Security Support

1. PURPOSE ........................................................................................................................ 2
2. INTRODUCTION ............................................................................................................ 2
3. BACKGROUND ............................................................................................................... 3
3.1. Program Designation ....................................................................................................... 3
3.2. Program of Record Deployment Schedule ..................................................................... 3
3.3. Ongoing Single Supply Solution Extensions and Key Deployment Activities .......... 3
3.4. Technical SAP Environment and Components ................................................................ 3
4. SCOPE ............................................................................................................................. 4
4.1. Introduction ...................................................................................................................... 4
4.1.1. Information Assurance .............................................................................................. 5
4.1.2. Personnel, Physical and Operational Security .......................................................... 5
4.2. Information Assurance Guidelines ................................................................................ 5
4.3. Contractor Labor Hours Reporting .............................................................................. 5
5. PERFORMANCE REQUIREMENTS ............................................................................ 6
5.1. Information Assurance Compliance .............................................................................. 6
5.1.1. Work Activity: Information Assurance Compliance Support .................................. 6
5.2. Security Operations .......................................................................................................... 9
5.2.1. Work Activity: Security Support .............................................................................. 9
5.3. Reception Support ......................................................................................................... 10
5.3.1. Work Activity: Reception Support ........................................................................... 10
6. Information Assurance Training and Certification Requirements ................................. 12
7. Security ........................................................................................................................... 12
1. **PURPOSE**

Work to be performed under this contract will support the Navy Enterprise Resource Planning (ERP) Program Management Office in Annapolis, Maryland. The contractor’s efforts will focus on providing Information Assurance (IA) and Security Operations support for the Navy ERP technical solution.

2. **INTRODUCTION**

The mission of the Navy ERP Program is to standardize Navy business processes for key acquisition, financial, and logistics operations. The Navy ERP Program leverages business process re-engineering (BPR) activities using best business practices supported in the SAP ERP software suite. The SAP software is the Public Sector Industry Solution certified by the Joint Financial Management Improvement Program (JFMIP) for U.S. Government use. The system improves Navy leadership decision making, enabling more effective and efficient support of the war fighter by streamlining and standardizing how the Navy manages people, money, Programs, equipment and supplies. Specifically, Navy ERP:

- Facilitates an End-to-End solution for receiving requests for resources (funding, material, contracts, people, and projects) and for processing those requests to fulfillment.
- Replaces the stove-piped, legacy systems currently used for financial management, inventory management and industrial operations, with a single integrated software Program with modules that support organization functions.
- Enable managers and line personnel to rapidly determine operating force logistics needs.
- Responds rapidly to Engineering Change Proposals (ECPs), emerging technology or performance enhancements through the system's integrated database providing visibility and status of transactions.
- Reduces the overall cost to the Navy by applying proven industry best practices and processes and replacing legacy IT systems.

Navy ERP combines BPR and industry best practices, supported by commercial off-the-shelf software, and integrates all facets of Navy business operations, using a single database to manage shared common data. The Program enables Navy compliance with the Chief Financial Officers Act of 1990 and the Department of Defense (DoD) Information Assurance Certification and Accreditation Process.

Additional benefits of the Program include the delivery of transparent and timely financial information improving decision making and reducing business operating costs. Cost savings are realized by the retirement of redundant, stove-pipe, legacy IT systems, a reduction in supply inventories due to improved inventory management and visibility and increased business process efficiencies.

Including deployment to Naval Sea Systems Command’s (NAVSEA's) Working Capital Fund, the system is deployed to approximately 66,000 users at Naval Air Systems Command (NAVAIR), Naval Supply Systems Command (NAVSUP), Space and Naval Warfare Systems Command (SPAWAR), and other commands throughout the U.S. Navy.
Systems Command (SPAWAR) and NAVSEA. When the Program of Record (PoR) deployments are executed in Oct 2012, Navy ERP will serve more than 71,000 users and be used to manage 51 percent of the Navy's Total Obligation Authority (TOA).

3. BACKGROUND

3.1. Program Designation

Navy ERP is designated as an Acquisition Category I (ACAT I), Major Automated Information System (MAIS) within the DoD. The Navy ERP Program offers two major SAP solutions; financial and acquisition solution, and single supply solution. In September 2007 the Program achieved acquisition Milestone C and is now in the deployment phase of the Financial and Acquisition Solution which provides Navy Echelon II and Echelon III commands with a full suite of automated tools to perform their business functions. The Program is on schedule to meet Full Deployment criteria in August 2013. This functionality falls into 4 major categories:

- Finance (General Fund and Navy Working Capital Fund)
- Plant Supply
- Workforce Management
- Acquisition / Program Management

3.2. Program of Record Deployment Schedule

The Program completed its first significant deployment in October 2007. Since that time the solution has been deployed to additional Commands and sites on a regular schedule. Follow-on Operational Test and Evaluation (FOT&E) is currently scheduled for the November 2012 to January 2013 timeframe. Additional solution updates, functional changes (ECPs), and deployments to additional Navy Commands are incorporated into the Integrated Master Schedule.

3.3. Ongoing Single Supply Solution Extensions and Key Deployment Activities

Concurrent with the Command deployments described in the prior section, the Program is also currently focused on the continued deployment of the Single Supply Solution, which provides additional Supply Chain management functionality. The Single Supply Solution provides Wholesale and Retail Supply functionality for Naval Inventory Control Points (ICPs) and Fleet and Industrial Supply Centers (FISCs) and 29 partner sites.

The final two financial and acquisition deployments to Strategic Systems Programs (SSP) and Office of Naval Research (ONR) will occur on 1 October 2012.

3.4. Technical SAP Environment and Components
Navy ERP is housed at NAVAIR's Patuxent River, Md. Naval Air Station, with a similarly sized disaster recovery system at NAVAIR’s China Lake, California Naval Weapons Station. The SAP systems run on Oracle's (Sun) multi-domain enterprise class systems (M9000/SF25k) using Solaris Unix as the primary operating system. The production systems utilize approximately 450 CPU cores with 2.4 TB of total memory or approximately 430,000 SAP Application Performance Standard (SAPS). The middleware systems are comprised of a combination of webMethods and MQ Websphere also running on Oracle (Sun) platforms. The enterprise core component (ECC) production database is currently approximately 6.5 terabytes (TB).

The system is accessed via the Navy ERP portal which is based on SAP’s enterprise portal. The portal Java components run on Oracle's (Sun) hardware. The portal is constructed as a single-sign on Common Access Card (CAC) based solution. Power users are redirected from the portal to a Citrix system that runs the SAP Graphical User Interface (GUI). The Citrix environment is constructed on virtualized Windows operating system platforms.

The Program has adopted a three (3) year upgrade cycle for SAP Software to maintain state-of-the-art commercial technology architecture and capabilities. ECC 6.0 Upgrade efforts are started in 2Q FY12 with full production cutover currently targeted for June 2012. The first Upgrade effort will focus on a “technical” upgrade of the SAP software to the most current versions and enhancement packs. The technical upgrade will be followed by two subsequent annual “functional” upgrades where software code is optimized to enable performance improvements and re-engineered business processes.

Navy ERP currently manages and administers 138 Oracle databases located at the primary data center and 20 Oracle databases at the Disaster Recovery site. There are approximately 58 ABAP systems (ECC/BW/SCM) and 24 JAVA systems. The remaining databases are associated with PMT and ancillary applications.

The current Navy ERP production user population is approximately 66,000 named users and is expected to grow to approximately 71,000 named users when the Program of Record (PoR) deployments have completed. The production system experiences approximately 8-9% user concurrency at peak times. Current sustaining account management includes approximately 1,000 account actions per week that includes changes, activations, locking and terminations.

Jobs within the SAP systems are scheduled using the Tivoli scheduling automation tool. The system currently processes daily approximately 6,000 jobs within the production system and 4,000 jobs within the non-production systems.

Navy ERP connects to 48 separate external systems with approximately 500 different interfaces generating several gigabytes of interface traffic on a daily basis. In addition, Navy ERP provides for approximately 10 external web services. Total traffic flows are on the order of 1-3 gigabytes per day. Interfaces types range from near real time synchronous message based to File Transfer Protocol (FTP) batch.

4. **SCOPE**

   4.1. **Introduction**
4.1.1. Information Assurance

The purpose of this effort is to provide Information Assurance and Security Operations support services to ensure the Navy ERP solution is maintained and operated in accordance with applicable Information Assurance requirements, policies and best practices. This Defense-in-Depth (DiD) approach applies IA principles and controls regarding people, processes and technology to safeguard the Navy ERP system against cyber attacks, whether internal or external. Coordination with internal and external Navy ERP support teams is critical to effectively analyze vulnerabilities, assess risk and identify effective mitigation to protect the Navy ERP Information Technology system. These efforts must be provided as needed, with minimal or no delay. The Navy ERP System capability is available 22.8 hours daily, from a user standpoint, to support Global Combat Support System (GCSS) Family of Systems requirements. This requirement factors 1.2 hours/day of average downtime, which represents both scheduled and unscheduled downtime, yielding an operational availability (Ao) of .95.

All Information Assurance work activities and deliverables will be authorized and approved by the Information Assurance Manager for the Navy ERP System Government Lead or their designee.

4.1.2. Personnel, Physical and Operational Security

Also part of this requirement is the personnel, physical and operational security support provided to the Government and contractor personnel who provide support to Navy ERP Program operations. All work activities and deliverables in this area will be authorized and approved by the Navy ERP Program Deputy Chief of Staff.

4.2. Information Assurance Guidelines

The purpose of the Department of the Navy (DON) IA Program is to protect information to support the DON mission as described in the DON Information Management and Information Technology (IM/IT) Strategic Plan, to “deliver secure, interoperable, and integrated information management and information technology to the Marine and Sailor to support the full spectrum of warfighting and warfighting support missions.” The major elements of the DON IA Program are: to promulgate IA policies and procedures to manage risk to DON IT assets, promote implementation of IA throughout the life cycle of all DON IT assets, and to integrate IA controls throughout the daily activities of the DON.

4.3. Contractor Labor Hours Reporting

The contractor shall report ALL contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for the Space and Naval Warfare Systems Command via a secure data collection site. The contractor is required to completely fill in all required data fields using the following web address https://doncmra.nmci.navy.mil.

Reporting inputs will be for the labor executed during the period of performance during each Government fiscal year (FY), which runs October 1 through September 30. While inputs
may be reported any time during the FY, all data shall be reported no later than October 31 of each calendar year. Contractors may direct questions to the help desk, linked at https://doncmra.nmci.navy.mil.

5. PERFORMANCE REQUIREMENTS

The contractor shall perform the following Information Assurance support related work activities in accomplishing the requirements of this Contract.

5.1. Information Assurance Compliance

5.1.1. Work Activity: Information Assurance Compliance Support

5.1.1.1. Key Personnel
- Senior Computer Security System Specialist
- Intermediate SAP Role Security Specialist

5.1.1.2. Objectives
Provide oversight, analysis and reporting to verify that Navy ERP technology hardware, systems software, SAP solution and components software and custom code are developed, installed, configured, maintained, and operated in accordance with all relevant and applicable Information Assurance requirements, policies and best practices. This includes policies and best practices related to personal information, data center facilities, and systems technical policies, regulations, and directives.

5.1.1.3. Work Activity:

5.1.1.3.1. Support activities that protect Navy ERP systems and sensitive Program data by organizing a robust IA Program that is staffed by technically competent IA personnel who possess appropriate Information Assurance certifications as required by DoD Manual 8570.01-M, Table AP3.T2.

5.1.1.3.2. Perform oversight and reviews of the Navy ERP system’s IA security posture that leads to a secure Navy ERP architecture that is compliant with the Global Information Grid (GIG) (compliance requirement IAW Homeland Security Presidential Directives (HSPD), Homeland Security, National Institute of Standards and Technologies (NIST), DoD, DON, and other Federal Security requirements). Advise the Government in methods and techniques for providing continuous IA security upgrades and meeting evolving requirements from DoD, DON, and other Federal Government agencies. Provide support to ensure these upgrades and requirements are appropriately managed and implemented, keeping Navy ERP in compliance with applicable policies and best practices for secure information technology system operations.

5.1.1.3.3. Analyze requirements and provide reports to the Government regarding all certification and accreditation activities necessary for
achieving and maintaining the Navy ERP system’s existing Authorization to Operate (ATO), in accordance with DoD Information Assurance Certification and Accreditation Process (DIACAP) requirements in DoDI 8510.01, and Federal Information Security Management Act (FISMA) of 2002, respectively. Develop security control test plans IAW aforementioned Federal standards and document results in the appropriate IA documentation. A certified Navy DIACAP Validator is required to coordinate this task, in accordance with SECNAV M-5239.2.

5.1.1.3.4. Conduct and support periodic reviews related to Information Assurance and Information Security related topics against all systems components, software, and configurations.

5.1.1.3.5. Support the Government in communicating Navy ERP IA requirements to all customer commands and developing precise instructions to promote efficiency and effectiveness in the successful fulfillment of these requirements. Ensure proper system usage by foreign national partners with verification from Command Business Offices.

5.1.1.3.6. Support the Government in conducting periodic system reviews and audits to ensure that systems security mechanisms, features, and configurations are working effectively to appropriately separate users from objects and data in accordance with defined roles and systems security policy.

5.1.1.3.7. Facilitate the running of current Defense Information Systems Agency (DISA) vulnerability scan tools against system servers, provide remediation and mitigation oversight, and report on residual vulnerabilities and risks.

5.1.1.3.8. Conduct and support the planning and execution of Navy ERP’s established Role Test Process using the existing set of Program database(s), documentation, and/or tools. Perform IA negative role testing and maintain the sensitive data matrix, Report results and recommend updates as applicable.

5.1.1.3.9. Support the Government in the coordination of information assurance requirements as they impact IT architecture with the Data Center security representatives, IT Team members and system administrators.

5.1.1.3.10. Ensure compliance with Information Assurance Vulnerability Management (IAVM) by coordinating patches, mitigations and responses, and reporting compliance status in the On-line Compliance Reporting System (OCRS), including preparation of mitigation plans.

5.1.1.3.11. Conduct reviews of technical design data to verify compliance with IA policies and best practices for the secure implementation of ERP systems. Remain vigilant and aware of changes in emerging IA requirements and threats to effectively participate in Program configuration control boards, such as the
Configuration Control Board (CCB), Configuration Management Board (CMB), Technical Change Control Board (TCCB), design document reviews and the User Management Working Group (UMWG).

5.1.1.3.12. Support the planning and execution of the annual Continuity of Operations Exercise (COOPEX) to verify that IA related requirements are met and the system is prepared for emergency situations.

5.1.1.3.13. Support the Privacy Officer in the task of ensuring that privacy policies are properly implemented and that breaches are properly reported in Navy ERP as required by DON Chief Information Officer (CIO) and other Federal Authorities.

5.1.1.3.14. Conduct and support reviews related to Information Assurance and Information Security of the Navy ERP System Interface Control Agreements (ICAs).

5.1.1.4. Deliverables

5.1.1.4.1. Reports on all IA compliance activities related to any SAP or non-SAP system in the Navy ERP system portfolio. Activities include role development decisions in the User Management Working Group (UMWG), configuration management reviews, the review of functional design documentation, review and updates to the Sensitive Data Matrix, User Access Requests and documentation associated with other IA-related issues. Quality of reports will be assessed based on coverage of the technical IA compliance and administrative components of the system and structured discipline of reports to include current accomplishments against planned work, unplanned work, and the plan for next week and any outstanding future IA critical tasks (regardless of party responsible for execution) - Weekly

5.1.1.4.2. A comprehensive IA Compliance report that covers all the major areas of the IA posture of the system and current/future compliance requirements based on Program, DON, DoD or other Government policies. This report shall provide insight for technical and budget planning on IA compliance efforts for the next three years. This report shall be delivered six months after contract award and updated annually, or as required to incorporate significant technology changes.

5.1.1.4.3. Reports on any system or data incident which includes findings and recommendations for reducing the risks and vulnerabilities leading to such incidents. Quality of reports will be assessed based on coverage of the technical components of the issue and impacts to compliance requirements, as well as, a structured discipline of the report to include the root cause and impact analysis, proposed
preventative measures, and final recommendations for process and system improvements.

5.1.1.4.4. Reports that are necessary to achieve and maintain a current system accreditation and full ATO. This includes FISMA vulnerability and mitigation reports. In addition, a comprehensive Security Test and Evaluation (ST&E) report must be produced and submitted to the Operational Designated Approving Authority (ODAA), as required. At least every three years a complete DIACAP accreditation package must be completed and submitted to the ODAA resulting in a successful accreditation and granting of an ATO. The current ATO expires 30 June 2013. A critical component of the DIACAP accreditation package is an updated Privacy Impact Assessment. Documentation of support activities necessary to maintain compliance with the Navy ERP system ATO letter is critical and must be maintained weekly.

5.1.1.4.5. Other identified document updates, compliance and exception reporting as deemed necessary by the Navy ERP Program, DON, DoD, and other applicable Government organizations. These include, but are not limited to the existing IA Acquisition Strategy, the Incident Response Plan, the IA Personnel Security Plan, the IAVM Plan, the IA Audit Review Plan and other required documentation and plans. This effort also includes reporting IAVM activity in the On-line Compliance Reporting System (OCRS).

5.1.1.4.6. Documentation and weekly status reports that capture IA support for Program or system support, responses to queries from other organizations, or reports and forms necessary to maintain system IA compliance.

5.1.1.4.7. Comprehensive report detailing the results of the Navy ERP System ICA reviews. – Quarterly

5.2. Security Operations

5.2.1. Work Activity: Security Support

5.2.1.1. Key Personnel

- N/A

5.2.1.2. Objective

Provide Personnel, Information and Security support to the Command Security Manager (CSM) ensuring the safety and security of all Program personnel, assets and facility by supporting the implementation and delivery of DOD security requirements in the following security disciplines: Personnel Security, Information Security, Physical Security and Operational Security.

Work Activities

5.2.1.2.1. Use the Joint Personnel Adjudication System (JPAS) to verify Program Office staff and visitor personnel security investigations.
5.2.1.2.2. Send, receive and log Visit Requests and Visit Authorization Letters with organizations manually and within JPAS.

5.2.1.2.3. In conjunction with the Information Assurance Team, assist Navy ERP Program Office leads in identifying position sensitivity, preparing forms to initiate personnel security investigations, tracking progress in JPAS, and notifying personnel and management of investigation results when available.

5.2.1.2.4. Assist Navy ERP prime and sub-contractor security officers navigate JPAS, understand facility clearance forms (DD-254) and IT Level investigation requirements and DoD Security Policies and Procedures.

5.2.1.2.5. Provide control of CACs and ensure returned cards are turned in at a DEERS/RAPIDS location.

5.2.1.2.6. Develop and execute procedures for enforcing DoD and Navy security regulations, including visitor control and staff identification (if required in addition to the Common Access Card (CAC)) to include Foreign National visitors which must be vetted through the Foreign Disclosure Office. Manage and monitor the facility badge system, the gate access system, and the facility surveillance system.

5.2.1.2.7. Monitor personnel within Program facilities, ensuring identification badges (or CACs) are properly secured and displayed. Develop and provide annual security and specialized training for Navy ERP Program Office staff and Contractor Verification System (CVS) Trusted Agents, especially regarding Foreign Nationals.

5.2.1.2.8. Develop continuity of operations plans, occupant emergency plans and other force protection plans in accordance with current policies in support of all COOP activities.

5.2.1.2.9. Maintain access lists and databases on all issued items and access-related information including restricted areas and intrusion detection.

5.2.1.2.10. Support the IAM by monitoring the facility wireless local area network for threats, rogues, unsuccessful logons, etc.

5.2.1.2.11. Review, update, and manage required Personnel IA/Security databases (i.e. TWMS – Total Workforce Management System) to include uploading new contractor personnel, new government personnel, and training certificates.

5.2.1.3. Deliverables

5.2.1.3.1. Personnel Security Access and Violation Reports – Monthly

5.2.1.3.2. Occupant Emergency Plan – Annually or As Required due to security requirements changes or Program needs.

5.3. Reception Support

5.3.1. Work Activity: Reception Support

5.3.1.1. Key Personnel
5.3.1.2. **Objective**

Provide facility reception support in the following disciplines: facility access, mail distribution and switchboard operations.

5.3.1.3. **Work Activities**

5.3.1.3.1. Ensure logging and clearance verification of all non-Navy ERP employees in compliance with Navy ERP policy, to include visitor/temp badge management, and reporting of badge discrepancies to Navy ERP Security.

5.3.1.3.2. Perform switchboard operations and maintain a telephone directory of the Navy ERP PMO.

5.3.1.3.3. Perform official mail distribution to include: maintaining policies and procedures for security and distribution of mail pick-up and delivery.

5.3.1.3.4. Manage all conference room scheduling for Navy ERP.

5.3.1.4. **Deliverables**

- N/A
6. **Information Assurance Training and Certification Requirements**

IA Personnel must hold a current DoD-approved Information Assurance certification as an IAM Level III as identified in the DoD Manual 8570.01-M policy.

7. **Security**

The nature of this task requires access up to SECRET information. The work performed by the contractor shall include access up to SECRET data, information, and spaces, as delineated in the DD-254. The contractor shall be required to attend meetings classified up to the SECRET level. The contractor shall be required to access business sensitive information.

If foreign travel is required, all outgoing Country/Theater clearance message requests shall be submitted to the SSC Pacific Foreign Travel Team, OTC2, Rm 1656 for action. A Request for Foreign Travel form shall be submitted for each traveler, in advance of the travel, to initiate the release of a clearance message at least 40 days in advance of departure. Each Traveler must also submit a Personal Protection Plan and have a Level 1 Antiterrorism/Force Protection briefing within one year of departure and a country specific briefing within 90 days of departure.

This demands certain actions by all members of the Navy ERP Program Team, including Government employees, consultants, and contractors. Business sensitive information must be protected from unauthorized disclosure. Further, the integrity of business sensitive information must be maintained. These must occur both at rest and in transit. For that reason, the contractor is required to meet the following:

1. All contractor personnel assigned to the Navy ERP Program must, as a minimum, meet the following requirements prior to assignment:
   a. U. S. Citizenship is required. Dual Citizenship is not authorized under any circumstance.
   b. IA personnel will be designated as IT-I, Critical-Sensitive, and must be the subject of a favorably adjudicated Single Scope Background Investigation (SSBI).

2. Upon assignment, all contractor personnel shall complete the following:
   a. DoD Information Assurance Awareness training for the current fiscal year as prescribed by Commander, Naval Network Warfare Command (NETWARCOM). Prior completion during the current fiscal year is acceptable if evidenced by a formal certificate.
   b. Obtain a DoD-issued Common Access Card (CAC)
c. Execute an OPNAV Form 5239/14, System Access Authorization Request – Navy (SAAR-N)
   d. Obtain building access cards as needed

3. The contractor shall provide a corporate e-mail account for each employee assigned to the Navy ERP Program. Each employee assigned to the Navy ERP Program shall digitally sign, using the Government furnished CAC, all e-mail used for official Government business and encrypt all e-mail used for official Government business that contains Controlled Unclassified Information (CUI - FOUO, Business Sensitive Information, Privacy Act, NOFORN, etc.). Further, the contractor shall ensure that data at rest on all assets used for digital storage of Government-owned information is encrypted using FIPS 140-2 certified encryption software.