

**Performance Work Statement (PWS) for Process Improvement,
Reengineering, Management and Data Support Services 2 (PIRMDS2)
for Service Delivery Model (SDM) Process Improvement Support**

1.0 Introduction:

NAVSUP Business Systems Center (BSC) plans to create a new Service Delivery Model (SDM), a Program Office for maintenance of the SDM, and the associated change management plan required to roll out the new model. The SDM will be geared towards ensuring support across multiple project types, technologies, funding sources and customers. This requirement includes a set of tools and processes that will support optimal delivery of Information Technology (IT) solutions while better supporting Navy Financial Auditability requirements. Additionally, the new NAVSUP BSC SDM will set standards that allow NAVSUP BSC to adapt faster to rapidly changing technologies as well as enable the NAVSUP BSC workforce to better position itself to take advantage of desirable business opportunities. NAVSUP BSC requires contractor support services (CSS) to provide support towards these goals.

2.0 Background:

In the past, NAVSUP BSC was successful in creation and adoption of the Software Process Improvement (SPI) methodology geared toward a standardized and repeatable set of process models in the sustainment and development of IT systems. With a dramatic shift of technology, NAVSUP BSC now supports a large SAP Enterprise Resource Planning (ERP) instance, numerous custom web-based applications, a mix of data appliances, large-scale mainframe applications and an assortment of Commercial-Off-The-Shelf (COTS) tools. With this shift, there is opportunity for NAVSUP BSC to move to a new SDM that better supports current and future workload.

2.1 Requiring Organization:

NAVSUP Business Systems Center
Code 92
5450 Carlisle Pike Bldg 409
Mechanicsburg, PA 17055

2.2 Project Description:

The purpose of this PWS is to secure support required to evaluate existing NAVSUP BSC standards, obtain recommendations based on proven industry-leading approaches, and to obtain guidance on and roll out of how to best adopt and incorporate new standards into NAVSUP BSC business processes. Furthermore, this project will provide needed support capable of translating

findings and recommendations into a new NAVSUP BSC SDM and introduce new toolsets, which will detail a repeatable and standardized delivery model that support multiple technical approaches for a diverse technology/customer/funding base. All required supporting processes will be documented thoroughly to ensure knowledge sharing and support Navy Financial Auditability requirements. In addition, training on all findings and recommendations with a focus on change management will be provided to the NAVSUP BSC employee workforce.

3.0 Scope:

As stated above, the goal of this PWS is to obtain contractor support services to help NAVSUP BSC identify, document and adopt proven approaches that will lead to consistent, predictable and reliable solution development and service delivery that is in full compliance with Financial Auditability requirements. In order to accomplish this, contractor support services are required to provide the following:

- Analysis and support services
- Mentoring and knowledge transfer

Effort success demands a common complement of methods, tools, architectures and metrics to ensure NAVSUP BSC's multidisciplinary teams can more effectively collaborate when providing support and working on customer IT solutions.

Moving to a standard and repeatable process model will benefit the Enterprise in the following ways:

- Create consistency across multiple business areas, allowing for easier transition between projects and more effective short-term resource sharing
- Provide cost avoidance through more effective early error detection, management of change, and prevention of re-work common in less structured delivery models
- Optimize business processes in concert with industry best IT process improvement principles to ensure improved processes appropriately address Audit requirements that begin for the Navy in Fiscal Year (FY) 2017
- Ensure compliance with industry leading processes/standards as set forth within the Project Management Body of Knowledge (PMBok®) Guide, Business Analysis Body of Knowledge (BABOK®) Guide, and the Software Engineering Body of Knowledge (SWEBoK®) Guide

4.0 Directives:

The Contractor shall comply with the following directives, and any updated/future versions as they are released:

- SECNAV Instruction M5510.30B Department of the Navy Personnel Security Program, 6 October 2006
- DoD Instruction 8500.01 Cybersecurity, 14 March 2014
- DoN Federal Information Security Management Act (FISMA) Guidance, March 2006
- DoD Directive (DoDD) 8570.1-M, 19 December 2005 (incorporating Change 3, 24 January 2012), Information Assurance Training, Certification and Workforce Management (will be superseded by DoDD 8140 Cyberspace Workforce Management)
- SECNAV Manual 5239.2 DoN Information Assurance Workforce Management, June 2016
- Department of Defense (DoD) Instruction 4161.02 - Accountability and Management of Government Contract Property, 27 April 2012
- DoD Instruction 8510.01 Risk Management Framework (RMF) for DoD Information Technology, 12 March 2014 (incorporating Change 1, 24 May 2016)
- Project Management Body of Knowledge (PMBok®) Guide, Fifth Edition
- Business Analysis Body of Knowledge (BABOK®) Guide, Version 3
- Software Engineering Body of Knowledge (SWEBoK®) Guide, Version 3
- NIST Special Publications 800-53, 800-53A, and 800-37 Revision 1
- NAVSUP BSC SDM, 2006

Formatted: Bulleted + Level: 1 + Aligned at: 0.25" + Indent at: 0.5"

5.0 Requirements/Tasks: ~~The contractor shall be obligated contractually to perform every requirement in this performance work statement. Not every performance requirement has a related standard expressed in this document. In such cases the performance standard is either inherent in the requirement or performance is to be in accordance with standard commercial practice.~~

~~Per 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. In addition, contractor~~

~~personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.~~

5.1 Analysis and Support Services. The Contractor shall perform and demonstrate the following tasks with/to designated NAVSUP BSC personnel:

- 5.1.1 Analyze the current NAVSUP BSC Service Delivery Model (SDM), complete a full assessment and devise an improved NAVSUP BSC SDM, based on existing industry-leading models, that provides a set of standardized and repeatable processes in the sustainment and development of IT systems, allowing for effective early error detection, management of change and prevention of re-work common in less structured delivery models:
- 5.1.1.1 Provide weekly updated SDM Evaluation Tracking and Effectiveness POAM in Microsoft Excel identifying steps, milestones, target completion dates, and progress made in completion of each step required to fully assess the NAVSUP BSC SDM as well as Key Performance Indicators (KPIs) intended to adequately monitor the overall effectiveness of the new SDM.

Performance Standard: SDM Evaluation Tracking and Effectiveness POAM must be ~~100~~99% error free and ~~100~~99% accurate. POAM must contain all required data as detailed within 5.1.1.1 100% of the time, and be provided to the Technical Assistant (TA) weekly 100% of the time in Microsoft Excel.

Assessment Method: TA review.

- 5.1.1.2 Provide a new NAVSUP BSC SDM, based on industry-leading standards in Microsoft Word that supports all standardized business areas that support IT Sustainment and Development efforts.

Performance Standard: NAVSUP BSC SDM must be 99% error free and 99% accurate. NAVSUP BSC SDM must contain all required data as detailed within 5.1.1.2 100% of the time, and be provided to the TA in Microsoft Word.

Assessment Method: TA review.

5.1.2 Evaluate NAVSUP BSC's existing processes for determining the best IT Solution, evaluating customer requirements, tracking project financial data, and sharing of resources:

5.1.2.1 Provide an IT Solution Evaluation Matrix in Microsoft Word that will assist NAVSUP BSC personnel in effectively evaluating new requirements and determining the most appropriate toolset/technology to be utilized.

Performance Standard: IT Solution Evaluation Matrix must be 99% error free and 99% accurate. IT Solution Evaluation Matrix must contain all required data as detailed within 5.1.2.1 100% of the time, and be provided to the TA in Microsoft Word.

Assessment Method: TA review.

5.1.2.2 Provide a Customer Evaluation Criteria Review Checklist in Microsoft Word that will assist NAVSUP BSC personnel in effectively evaluating customers' requirements at the outset of a project effort.

Performance Standard: Customer Evaluation Criteria Review Checklist must be 99% error free and 99% accurate. Customer Evaluation Criteria Review Checklist must contain all required data as detailed within 5.1.2.2 100% of the time, and be provided to the TA in Microsoft Word.

Assessment Method: TA review.

5.1.2.3 Provide Financial Auditability Process Documentation Guide in Microsoft Word that will assist NAVSUP BSC in tracking and monitoring project costs throughout the project lifecycle and will provide an auditable financial checklist template that meets FY 2017 U.S. Navy Financial Audit Tracking requirements and complements DoD IT Risk Management Framework (RMF) reporting requirements.

Performance Standard: Financial Auditability Process Documentation Guide must be 99% error free and 99% accurate. Financial Auditability Process Documentation Guide must contain all required data as detailed within 5.1.2.3 100% of the time, and be provided to the TA in Microsoft Word.

Assessment Method: TA review.

5.1.2.3.1 Provide a filled in Example Auditable Financial Checklist for a real NAVSUP BSC project in Microsoft Word.

Performance Standard: Example Auditable Financial Checklist must be ~~100~~99% error free and ~~100~~99% accurate. Example Auditable Financial Checklist must contain all required data as detailed within 5.1.2.3.1 100% of the time, and be provided to the TA in Microsoft Word.

Assessment Method: TA review.

5.2 Mentoring and Knowledge Transfer Services. The contractor shall actively provide daily mentoring and training support for the NAVSUP BSC employee workforce to ensure government employees are provided with the required knowledge in implementing Change Management needed to adhere to and implement actions required to administer the updated NAVSUP BSC SDM and additional documentation provided as part of Section 5.1.

5.2.1 Expert Transfer:

5.2.1.1 Provide a minimum of five (5) Change Management workshops for the NAVSUP BSC employee workforce that will enable employees to better manage change.

Performance Standard: Change Management workshops must be ~~100~~99% error free and ~~100~~99% accurate. Change Management workshops must provide all information as detailed within 5.2.1.1 100% of the time.

Assessment Method: TA review.

5.2.1.2 Provide weekly updated Mentoring and Knowledge Transfer Update Log that tracks progress in Microsoft Excel and identifies exact mentoring activities and knowledge transferred, including schedule for and

progress in completion of change management workshops presented, topics covered, attendees, progress in completing documentation listed within Section 5.1, including milestones, target completion dates, and progress made in completion of each step required to transfer knowledge.

Performance Standard: Mentoring and Knowledge Transfer Update Log must be 100% error free and 100% accurate. Mentoring and Knowledge Transfer Update Log must contain all required data as detailed within 5.2.1.2 100% of the time, and be provided to the TA weekly 100% of the time in Microsoft Excel.

Assessment Method: TA review.

6.0 Deliverables: All deliverables must meet the format requirements specified by the Contracting Officer's Representative. Documentation related to these services shall be made available electronically. The following list details the contract deliverables:

6.1 Monthly Status Reports. Status reports shall be sent electronically to the Technical Assistant (TA) and Contracting Officer's Representative (COR) within seven (7) days following the end of the monthly period. The monthly status report shall include the following elements:

- List of completed actions such as requirements gathering sessions, customer support, or other meetings with BSC personnel.
- Any issues/problems encountered and recommended solutions.
- Progress on required documentation.

6.2 Provide SDM Evaluation Tracking and Effectiveness POAM as specified in Paragraph 5.1.1.1.

6.3 Provide new NAVSUP BSC SDM in compliance with the specifications detailed in Paragraph 5.1.1.2.

6.4 Provide IT Solution Evaluation Matrix in compliance with the specifications detailed in Paragraph 5.1.2.1.

- 6.5 Provide Customer Evaluation Criteria Review Checklist in compliance with the specifications detailed in Paragraph 5.1.2.2.
- 6.6 Provide Financial Auditability Process Documentation Guide in compliance with the specifications detailed in Paragraph 5.1.2.3.
- 6.7 Provide Example Auditable Financial Checklist in compliance with the specifications detailed in Paragraph 5.1.2.3.1.
- 6.8 Provide Mentoring and Knowledge Transfer Update Log in compliance with the specifications detailed in Paragraph 5.2.1.2.

Unless stated otherwise, the following instructions apply to all deliverables:

- All versions of the deliverables required by the TO shall be delivered electronically to the COR and/or his/her designee and shall be subject to Government review and approval.
- Deliverable due dates shall take into account the review periods described below.
 - o Draft deliverables will be reviewed and feedback and/or requested changes provided within 7 business days (unless otherwise specified).
 - o Government reserves the right to request a formal review session with the contractor during these timeframes and may request that the contractor make changes to any version of a deliverable.
 - o Government will review and approve or reject all final versions of all deliverables within 7 business days of receipt (unless otherwise specified).
 - o If any deliverable is rejected, the contractor will be notified within the specified time periods and will have 7 calendar days within which to rework the deliverable and resubmit for Government approval. All changes to any version of a deliverable and/or deliverable outline shall be approved by the COR. If more than the specified number of calendar days is required for Government review and approval, the COR will inform the contractor of the need for an extension within the initial review period.
 - o Contractor shall prepare and submit the deliverables on or before the required due date to the COR or designee via email. For deliverables that are not documents the contractor shall submit a description of the deliverable and any associated

documentation or descriptive information. In no case shall any deliverable be received by the Government less than 21 calendar days prior to the end of the Period of Performance.

o Rejection of any deliverable by the Government does not excuse the contractor from meeting the baseline due dates for any other deliverables.

7.0 Period of Performance:

Work shall be performed from the Date of Award (DOA) for 12 months with one 12-month option requested. ~~JK (Delete per KH) Performance shall occur Monday through Friday between 6am and 6pm. Some flexibility in daily hours is permitted with the TA's approval. No contractor services shall be performed Saturdays, Sundays, Government Holidays or during base closures without prior approval from the TA.~~ The contractor shall follow Naval Support Activity Mechanicsburg base policy for reporting to work during severe weather and base closure. The contractor is not authorized to begin work until both the Visit Authorization Request (VAR) and System Authorization Access Request (SAAR) forms have been successfully processed and base and system access have been granted.

~~START-UP PERIOD (JK Delete and revise per KH)~~

~~It is intended to make award of the resultant contractual vehicle in time to allow an approximate 30 day start up period in advance of the actual commencement of the performance period. All contractor resource onboarding documents must be submitted via the prime contractor. The prime contractor shall make all necessary preparations, during this start up period, to assume full responsibility for productive performance as of the performance start date (unless a transition period is called out in this PWS, then full responsibility shall be assumed after the transition period).~~

Definition of "productive": ON-BOARDING PROCESS

All contractor resource onboarding documents must be submitted via the prime contractor. An employee is considered to be "productive" upon completion of the following items:

- a. Visit Authorization Request (VAR)
- b. Contractor Information Sheet (CIS)
- c. FD-258 fingerprint card
- d. Completed EQIP (Electronic Investigation) within 20 days after contract award
- e. All contractor resource(s) must have an active JPAS profile within 20 days after contract award

- f. Common Access Card (CAC)
- g. System Authorization Access Request - Navy (SAAR-N)
- h. Cyber Awareness Training Certification
- i. Information Assurance (IA) certification (if applicable)
- j. User Access Request (UAR) Only applies when contractor requires access to ERP/SAP (Contractor does not require this access.)

Note (1): Invoicing by the contractor will begin as of the commencement of the performance period of services. ~~and no reimbursement will be paid by the Government for efforts expended during the start-up period.~~

Note (2): Dual Citizenship and Foreign Nationals are not allowed access to the functional/system side of ERP/SAP.

Contractor and subcontractor employees performing under this task order are required to sign a Non-disclosure Agreement (NDA) as part of their onboarding process. Refer to DFARS 252.204-7000, Disclosure of Information, and DFARS 252.204-7003, Control of Government Personnel Work Product.

8.0 Place of Performance:

The NAVSUP BSC, Mechanicsburg, PA is the primary site for performance. Work may be performed remotely at the contractor facility with prior approval of the Technical Assistant Point of Contact (TAPOC).
~~Predominantly, work will be performed in NAVSUP BSC work spaces in Mechanicsburg PA. Work may be performed remotely at the contractor facility with prior approval of the Technical Assistant (TA).~~

9.0 Travel:

Travel is not required.

10.0 ~~10.0~~ Security:

Per 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. In addition, contractor personnel shall appropriately identify themselves as contractor employees in telephone conversations and in formal and informal written correspondence.

Formatted: No bullets or numbering

Comment [kbh1]: If a contractor proposes to perform 100% of this task order at their facility is that going to meet your requirements? No, we need the resources onsite, at least part of the time to work with the project teams directly.

Alternately, if a contractor proposes 100% of their personnel to be on-site at Mechanicsburg do you have the capacity to accommodate this? Yes, this will be great.

Comment [kbh2]: Again, TPOC does not have this type of authority.

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 6 + Alignment: Left + Aligned at: 0" + Indent at: 0.5"

Formatted: Indent: Left: 0.5"

5252.204-9400 Contractor Unclassified Access to Federally Controlled Facilities, Sensitive Information, Information Technology (IT) Systems or Protected Health Information (July 2013)

Homeland Security Presidential Directive (HSPD)-12, requires government agencies to develop and implement Federal security standards for Federal employees and contractors. The Deputy Secretary of Defense Directive-Type Memorandum (DTM) 08-006 – “DoD Implementation of Homeland Security Presidential Directive – 12 (HSPD-12)” dated November 26, 2008 (or its subsequent DoD instruction) directs implementation of HSPD-12. This clause is in accordance with HSPD-12 and its implementing directives.

APPLICABILITY

This clause applies to contractor employees requiring physical access to any area of a federally controlled base, facility or activity and/or requiring access to a DoN or DoD computer/network/system to perform certain unclassified sensitive duties. This clause also applies to contractor employees who access Privacy Act and Protected Health Information, provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Position, as advised by the command security manager. It is the responsibility of the responsible security officer of the command/facility where the work is performed to ensure compliance.

Each contractor employee providing services at a Navy Command under this contract is required to obtain a Department of Defense Common Access Card (DoD CAC). Additionally, depending on the level of computer/network access, the contract employee will require a successful investigation as detailed below.

ACCESS TO FEDERAL FACILITIES

Per HSPD-12 and implementing guidance, all contractor employees working at a federally controlled base, facility or activity under this clause will require a DoD CAC. When access to a base, facility or activity is required contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy Command and shall out-process prior to their departure at the completion of the individual's performance under the contract.

ACCESS TO DOD IT SYSTEMS

In accordance with SECNAV M-5510.30, contractor employees who require access to DoN or DoD networks are categorized as IT-I, IT-II, or IT-III. The IT-II level, defined in detail in SECNAV M-5510.30, includes positions which require access to information protected under the Privacy Act, to include Protected Health Information (PHI). All contractor employees under this contract who require access to Privacy Act protected information are therefore categorized no lower than IT-II. IT Levels are determined by the requiring activity's Command Information Assurance Manager. Contractor employees requiring privileged or IT-I level access, (when specified by the terms of the contract) require a Single Scope Background Investigation (SSBI) which is a higher level investigation than the National Agency Check with Law and Credit (NACLC) described below. Due to the privileged system access, a SSBI suitable for High Risk public trusts positions is required. Individuals who have access to system control, monitoring, or administration functions (e.g. system administrator, database administrator) require training and certification to Information Assurance Technical Level 1, and must be trained and certified on the Operating System or Computing Environment they are required to maintain.

Access to sensitive IT systems is contingent upon a favorably adjudicated background investigation. When access to IT systems is required for performance of the contractor employee's duties, such employees shall in-process with the Navy Command's Security Manager and Information Assurance Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The decision to authorize access to a government IT system/network is inherently governmental. The contractor supervisor is not authorized to sign the SAAR-N; therefore, the government employee with knowledge of the system/network access required or the COR shall sign the SAAR-N as the "supervisor".

The SAAR-N shall be forwarded to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

When required to maintain access to required IT systems or networks, the contractor shall ensure that all employees requiring access complete annual Information Assurance (IA) training, and maintain a current requisite background

investigation. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

INTERIM ACCESS

The Navy Command's Security Manager may authorize issuance of a DoD CAC and interim access to a DoN or DoD unclassified computer/network upon a favorable review of the investigative questionnaire and advance favorable fingerprint results. When the results of the investigation are received and a favorable determination is not made, the contractor employee working on the contract under interim access will be denied access to the computer network and this denial will not relieve the contractor of his/her responsibility to perform.

DENIAL OR TERMINATION OF ACCESS

The potential consequences of any requirement under this clause including denial or termination of physical or system access in no way relieves the contractor from the requirement to execute performance under the contract within the timeframes specified in the contract. Contractors shall plan ahead in processing their employees and subcontractor employees. The contractor shall insert this clause in all subcontracts when the subcontractor is permitted to have unclassified access to a federally controlled facility, federally-controlled information system/network and/or to government information, meaning information not authorized for public release.

CONTRACTOR'S SECURITY REPRESENTATIVE

The contractor shall designate an employee to serve as the Contractor's Security Representative. Within three work days after contract award, the contractor shall provide to the requiring activity's Security Manager and the Contracting Officer, in writing, the name, title, address and phone number for the Contractor's Security Representative. The Contractor's Security Representative shall be the primary point of contact on any security matter. The Contractor's Security Representative shall not be replaced or removed without prior notice to the Contracting Officer and Command Security Manager.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO NATIONAL SECURITY POSITIONS OR PERFORMING SENSITIVE DUTIES

Navy security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Navy recognizes contractor employees under this contract as Non-Critical Sensitive [ADP/IT-II] when the contract scope of work require physical access to a federally controlled base, facility or activity and/or requiring access to a DoD computer/network, to perform unclassified sensitive duties. This designation is also applied to contractor employees who access Privacy Act and Protected Health Information (PHI), provide support associated with fiduciary duties, or perform duties that have been identified by DON as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLIC to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The NACLIC consists of a standard NAC and a FBI fingerprint check plus law enforcement checks and credit check. Each contractor employee filling a non-critical sensitive or IT-II position is required to complete:

- SF-86 Questionnaire for National Security Positions (or equivalent OPM investigative product)
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date. Background investigations shall be reinitiated as required to ensure investigations remain current (not older than 10 years) throughout the contract performance period. The Contractor's Security Representative shall contact the Command Security Manager for guidance when reinvestigations are required.

Regardless of their duties or IT access requirements ALL contractor employees shall in-process with the Navy Command's Security Manager upon arrival to the Navy command and shall out-process prior to their departure at the completion of the individual's performance under the contract. Employees requiring IT access shall also check-in and check-out with the Navy Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Navy Information Technology resources. The SAAR-N shall be forwarded

to the Navy Command's Security Manager at least 30 days prior to the individual's start date. Failure to provide the required documentation at least 30 days prior to the individual's start date shall result in delaying the individual's start date.

The contractor shall ensure that each contract employee requiring access to IT systems or networks complete annual Information Assurance (IA) training, and maintain a current requisite background investigation. Contractor employees shall accurately complete the required investigative forms prior to submission to the Navy Command Security Manager. The Navy Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM). Suitability/security issues identified by the Navy may render the contractor employee ineligible for the assignment. An unfavorable determination made by the Navy is final (subject to SF-86 appeal procedures) and such a determination does not relieve the contractor from meeting any contractual obligation under the contract. The Navy Command's Security Manager will forward the required forms to OPM for processing. Once the investigation is complete, the results will be forwarded by OPM to the DON Central Adjudication Facility (CAF) for a determination.

If the contractor employee already possesses a current favorably adjudicated investigation, the contractor shall submit a Visit Authorization Request (VAR) via the Joint Personnel Adjudication System (JPAS) or a hard copy VAR directly from the contractor's Security Representative. Although the contractor will take JPAS "Owning" role over the contractor employee, the Navy Command will take JPAS "Servicing" role over the contractor employee during the hiring process and for the duration of assignment under that contract. The contractor shall include the IT Position Category per SECNAV M-5510.30 for each employee designated on a VAR. The VAR requires annual renewal for the duration of the employee's performance under the contract.

BACKGROUND INVESTIGATION REQUIREMENTS AND SECURITY APPROVAL PROCESS FOR CONTRACTORS ASSIGNED TO OR PERFORMING NON-SENSITIVE DUTIES

Contractor employee whose work is unclassified and non-sensitive (e.g., performing certain duties such as lawn maintenance, vendor services, etc ...) and who require physical access to publicly accessible areas to perform those duties shall meet the following minimum requirements:

- Must be either a US citizen or a US permanent resident with a minimum of 3 years legal residency in the United States (as required by The Deputy Secretary of Defense DTM 08-006 or its subsequent DoD instruction) and
- Must have a favorably completed National Agency Check with Written Inquiries (NACI) including a FBI fingerprint check prior to installation access.

To be considered for a favorable trustworthiness determination, the Contractor's Security Representative must submit for all employees each of the following:

- SF-86 Questionnaire for Non-Sensitive Positions
- Two FD-258 Applicant Fingerprint Cards (or an electronic fingerprint submission)
- Original Signed Release Statements

The contractor shall ensure each individual employee has a current favorably completed National Agency Check with Written Inquiries (NACI) or ensure successful FBI fingerprint results have been gained and investigation has been processed with OPM

Failure to provide the required documentation at least 30 days prior to the individual's start date may result in delaying the individual's start date.

* Consult with your Command Security Manager and Information Assurance Manager for local policy when IT-III (non-sensitive) access is required for non-US citizens outside the United States.

(End of Clause)

DoD 8570.01-M Information Assurance Workforce Improvement Program. (JK Keep this in for clarification.)

X No Additional IA Certification Required
 N/A Information Assurance DoD 8570.01-M Required:
 IA Certification Level N/A
 Computing Environment Certification N/A

Privileged system access is not required.

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. The Contractor shall meet the applicable information assurance certification requirements, including-

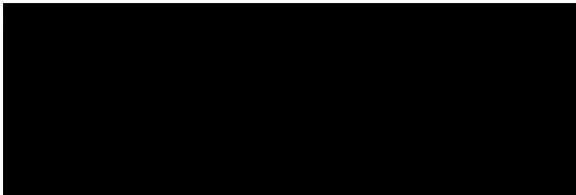
(1) DoD-approved information assurance workforce certifications appropriate for each category and level as listed in the current version of DoD 8570.01-M.

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

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

(b) 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.

Proof of the above indicated IA certification and computing environment certification is to be provided for all contractor personnel along with the vendor quote. In addition to the IA certificate, active enrollment and participation in the certification maintenance program must be established prior to contract award to ensure the appropriate access can be secured by contractor resources. All required IA and/or computing environment certifications must be current at the contract period start date; there is no "grace" period to obtain these certifications. Questions and additional information requirements may be addressed by contacting the NAVSUP Business Systems Center Information Assurance Manager (IAM).



11.0 Government Furnished Equipment:

The government will provide work facilities to the on-site contractor. The government will provide computer hardware and software required and access to local telephones with voicemail and long distance access when the contractor is acting on behalf of the government. NAVSUP Business Systems Center will provide all equipment, tools and servers used to maintain software and host these applications.

12.0 Qualifications/Experience:

The contractor personnel assigned shall possess the qualifications as stated in the base IDIQ and 1) Senior Systems/Operations Research Analyst must have at least five (5) years; 2) Senior Knowledge Management must have at least four (4) years, of the following:

- Experience and working knowledge in the area of implementing Change Management
- Functional and Technical experience working with IT
- Experience performing evaluations of or working with industry-leading IT organizational service delivery models
- Experience and working knowledge of IT best practices
- Experience and working knowledge of implementing and training in the area of Process Improvement

~~13.0-- Non-Disclosure Agreement: Moved to onboarding per KH~~

~~The Business Sensitive Information Non-disclosure Agreement is required for this order. Refer to DFARS-252.204-7000, Disclosure of Information, and DFARS-252.204-7003, Control of Government Personnel Work Product.~~

Formatted: Outline numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 12 + Alignment: Left + Aligned at: 0" + Tab after: 0.5" + Indent at: 0.5"

14.013.0 NAVSUP Business Systems Center Procedures for Contractor Access/Visit Authorization Request (VAR):

1. A company letter to the Technical Assistant (TA) containing the following information:

- a. Contract Information
 - (1) Contract Number
 - (2) Date Issued
 - (3) Date of Expiration
 - (4) Name and phone number of the TA
 - (5) Purpose
 - (6) Systems to be accessed

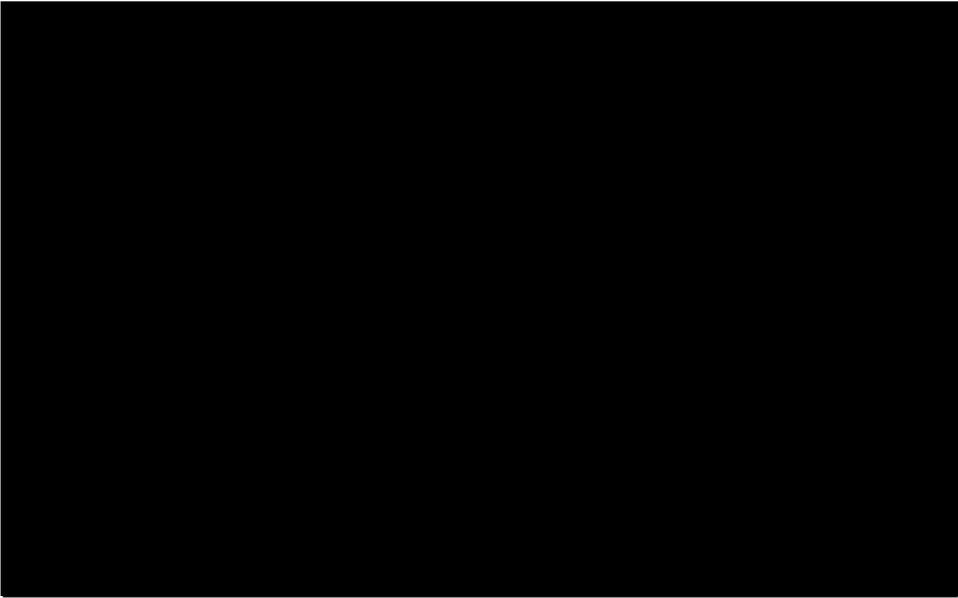
- (7) Files/Data required
- (8) Type of access required (i.e., inquiry/update/delete)
- (9) Equipment to be used with location and mode of access identified
- (10) Security point of contact including address and phone number

b. Information for all contractor employees requesting access, to include:

- (1) Full Name
- (2) Job Title
- (3) Date of Birth
- (4) Place of Birth
- (5) Citizenship
- (6) Social Security Number
- (7) Naturalization Number (if applicable)
- (8) Type and date of Security Investigation.
- (9) Government Clearance Level (if applicable)
- (10) Valid email address for the Contractor's employee

c. Appropriate Company Official's signature

2. A System Authorization Access Request Navy (SAAR-N) form (OPNAV 5239/14) with original signatures and a copy of the DOD Annual IA Awareness Training Completion Certificate for each contractor employee sent to the TA.



16-015.0 Enterprise-wide Contractor Manpower Reporting Application (ECMRA)

The contractor shall report ALL-contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract for SDM~~this effort~~ via a secure data collection site. Contracted services excluded from reporting are based on Product Service Codes (PSCs). The excluded PSCs are:

- (1) W, Lease/Rental of Equipment;
- (2) X, Lease/Rental of Facilities;
- (3) Y, Construction of Structures and Facilities;
- (4) D, Automatic Data Processing and Telecommunications, IT and Telecom-Telecommunications Transmission (D304) and Internet (D322) ONLY;
- (5) S, Utilities ONLY;
- (6) V, Freight and Shipping ONLY.

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>.

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"

Formatted: Indent: Left: 0.5"

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"

Formatted: List Paragraph, No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"

Formatted: List Paragraph, No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"

Formatted: List Paragraph, No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"

Formatted: List Paragraph, No bullets or numbering

Formatted: Numbered + Level: 1 + Numbering Style: 1, 2, 3, ... + Start at: 1 + Alignment: Left + Aligned at: 0.5" + Indent at: 1"

Formatted: List Paragraph, No bullets or numbering