

PERFORMANCE WORK STATEMENT
CONTINUED READINESS PROGRAM
AND
LIFE SAFETY ASSESSMENT
NAVAL HOSPITAL CAMP LEJEUNE, NC

SECTION 1 - GENERAL INFORMATION

Section 1.1 Scope

Services are required from a contractor to work directly with the Naval Hospital Camp Lejeune (NHCL), NC, to develop a Continued Readiness Program (CRP) by surveying approximately 552,000 gross square feet of healthcare occupancy at NHCL Building NH100. Contractor services shall be performed in accordance with The Joint Commission's (TJC) Environment of Care (EC)/Life Safety (LS) components. The Contractor shall perform an assessment of the LS Posture as it relates to the National Fire Protection Association (NFPA) 101 Life Safety Code (LSC) and will advise Camp Lejeune's Naval Hospital Facilities Department of any EC/LS/Emergency Management (EM) deficiencies in order to prepare for the unannounced Accreditation Survey by TJC. The Contractor shall perform PWS requirements at Camp Lejeune Naval Hospital, NC, and remainder of work shall be performed at the Contractor's facility.

Section 1.2 Period of Performance

The period of performance associated with this PWS shall be for a twelve (12) month base period and three (3) twelve (12) month option periods to be exercised at the option of the Government.

SECTION 2 – DESCRIPTION OF TASKS

Section 2.1 – Performed during Year 1, 2, 3, 4 of the CRP

2.1.1 The Contractor shall provide Camp Lejeune's Facilities Department a comprehensive and multiple audit process for the EC Program through the CRP. This process will consist of multiple Contractor on-site visits that include a comprehensive review of all Safety (SA), Security (SE), Fire Safety (FS), Hazardous Materials & Waste (HM), Medical Equipment (ME), and Life Safety Elements of Performance. The Contractor shall accomplish the audit process through compliance verification of records and documents including, but not limited to, all management plans, risk assessments, annual evaluations, EC/LS/EM Reporting & Committee Activities, and Performance Improvement Plans. Each scheduled Contractor visit includes a physical site evaluation consisting of random staff challenges in mock survey fashion combined with a hazard surveillance tour as well as following up on any issues noted on previous surveys.

2.1.2 The Contractor shall provide the following services:

- 2.1.2.1** Perform quarterly on-site assessment reviews consisting of four (4) weeks, sixteen (16) days each year. Provide an agenda for each visit to include morning briefings and an exit conference on the last day of the visit(s) with senior leadership, facilities, quality management and others as designated by the QM department
- 2.1.2.2** Review key EC/LS/EM records and documents such as management plans, annual evaluations, EC/EM Committee meetings minutes, performance measures, etc.
- 2.1.2.3** Random Records Review - examine a random selection of performance measures, hazard surveillance rounds, security records, training documentation, etc.
- 2.1.2.4** Perform physical site evaluations and risk assessment. Building tour of Patient and non patient care areas, construction sites, etc. The contractor will tour the facility during each visit, performing visual inspections and conducting random staff challenges (in mock survey fashion).
- 2.1.2.5** Assist in EC/LS program development and maintenance as applicable, and provide education throughout the process to assist Naval Hospital Camp Lejeune staff in understanding the EC/LS/EM process and requirements.
- 2.1.2.6** Provide a written report after each visit with 10 calendar days.
- 2.1.2.7** Provide follow-up on previously noted deficiencies to evaluate for sustained compliance.
- 2.1.2.8** Provide ongoing Joint Commission EC/LS/EM informational updates and other regulatory updates on site visits and in education.
- 2.1.2.9** Provide telephone support & guidance during the actual survey and meet on-site if possible or the Team Leader available by phone during the on site triennial survey.
- 2.1.3.0** Education and Training crosswalk regarding EC/LS/EM Joint Commission standards updates for clinical and non clinical staff and providers each visit (minimum of 4 times a year) Presentation and handouts to be provided one week prior to visit

Section 2.2 – Performed during Year 2 and Year 4 of the CRP

- 2.2.1** The Contractor shall provide a Statement of Conditions (SOC) Assessment document that includes a Plan For Improvement (PFI) and a cost estimate for

corrective actions. In addition, the Contractor will update Government drawings to reflect all of the following, but not limited to, on individual layers:

- Fire/Smoke Barrier Locations
- Smoke Compartments
- Distances to Exits
- Distances to Smoke Barriers
- Suites
- Hazard Area Locations

2.2.2 The Contractor shall identify the square footage of area used for healthcare from business or occupancies other than healthcare.

2.2.3 The Contractor will provide finalized drawings with a legend showing compliance with the suite and compartment rules per NFPA 101 2000 edition or most current adopted version.

2.2.4 The Contractor will perform an assessment of the NHCL, NC, Building NH100 in order to determine compliance with NFPA 101 Life Safety Code 2000 edition (or current adopted version) as prescribed by TJC Statement of Conditions Compliance Document.

2.2.5 The Contractor will develop deficiency drawings that will identify on the floor plans the locations of the actual deficiencies. Each deficiency must be labeled on the floor plan with a number. That number will correspond to a number on the detailed deficiency report. Deficiencies relating to rated doors, exit signs, vertical openings, fire extinguishers, fire alarm pull stations, audible/visual appliances, kitchen exhaust hood systems, means of egress, dead end corridors issues, and travel distance, and hazardous areas will be identified.

2.2.6 Upon completion of the survey, the Contractor will develop the Plan for Improvement (PFI) consisting of PFI groups and Lists of Deficiency by Type or Category. For each deficiency a unique identifier for tracking purposes and the specific location will be provided. In addition, the Contractor will provide a resolution section that includes a description of the proposed action, placement for contractor's name/in-house personnel name, and relevant dates of actions to be completed by the facility. The Government will assist with the electronic PFI (e-PFI) as needed.

2.2.7 The Contractor shall perform an assessment of NHCL Building NH100 to determine compliance with NFPA 101 LS Code 2000 edition as prescribed by TJC Statement of Conditions Compliance Document Parts 3A & 3B.

SECTION 3 - CONTRACTOR PERSONNEL

The contractor shall provide personnel that possess the necessary qualifications, skills, background, and expertise to perform in accordance with the requirements of this PWS. In addition, contractor personnel shall have knowledge of:

- The Joint Commission (TJC)
- Occupational Safety and Health Administration (OSHA)
- National Fire Protection Association (NFPA)
- American National Standards Institute (ANSI)
- Certified Healthcare Safety Professional
- Association for the Advancement of Medical Instrumentation (AAMI)
- ECRI Institute
- Hospital physical operations, fire safety/codes, emergency preparedness, building codes and environment of care readiness; and
- General maintenance/engineering, construction management/safety, regulatory compliance, communications, environmental services, biomedical services, emergency management, hazmat, fire safety, utilities, safety and security in healthcare facilities.

SECTION 4 - DELIVERABLES

The following table lists all required deliverables applicable to this contract:

Deliverable No.	Deliverable Description	PWS Reference Paragraph	Due Date	Copy To
1.	1 Copy of the Life Safety Plan Drawings in 11” X 17” Format (Electronic Format)	See Section 2.2	Aug. 15th 2017(TBD) Aug. 15th 2019 (TBD)	COR
2.	1 Copy of the Deficiency Drawings in 11” X 17” Format (Electronic Format)	See Section 2.2	Aug. 15th 2017(TBD) Aug. 15th 2019 (TBD)	COR
3.	1 Copy of the Detailed Deficiency Report with Preliminary Cost Estimates (Electronic Format)	See Section 2.2	Aug. 15th 2017(TBD) Aug. 15th 2019 (TBD)	COR

4.	1 Copy of the Plan for Improvement (PFI) in Excel Format (Electronic Format)	See Section 2.2	Aug. 15th 2017(TBD) Aug. 15th 2019 (TBD)	COR
----	--	-----------------	---	-----

SECTION 5 - GOVERNMENT FURNISHED INFORMATION (GFI)

The Government will make available copies of technical documentation, drawings, and magnetic media as appropriate, in support of task requirements. All GFI is provided for information purposes and remains the property of the Government. The following GFI is anticipated:

Drawings. Drawings in AutoCad (CAD) format for any additions, changes, or renovations, for use to incorporate in the facility's life safety drawings.

SECTION 6 - HOURS OF OPERATION

Normal working hours, 7:30AM – 4:00PM, Monday through Friday are anticipated under this contract excluding federal holidays. Services affected by holidays shall be performed on the next Government work day.

SECTION 7 - NON-PERSONAL SERVICES STATEMENT

Contractor employees performing services under this contract will be controlled, directed, and supervised at all times by management personnel of the Contractor. Contractor management will ensure that employees comply with the performance work standards outlined in this PWS. Contractor employees will perform their duties independent of, and without the supervision of, any Government official. The tasks, duties, and responsibilities set forth in the task may not be interpreted or implemented in any manner that results in any Contractor employee creating or modifying Federal policy, obligating the appropriated funds of the United States Government, overseeing the work of Federal employees, providing direct personal services to any Federal employee, otherwise violating the prohibitions set forth in Subparts 7.5 and 37.1 of the Federal Acquisition Regulation (FAR) <http://farsite.hill.af.mil/vffar1.htm>. The Government shall control access to the facility and shall perform the inspection and acceptance of completed work.

SECTION 8 - IDENTIFICATION REQUIREMENTS

All contractor personnel performing under this performance work statement shall identify themselves as a contractor employee to avoid creating any impression that they are Government officials. Such identification shall be made in all meetings attended, when answering Government telephones, on all e-mails, and when working in other situations where their

contractor status is not obvious to third parties. They must also ensure that all documents or reports produced by contractors are suitably marked as contractor products or that contractor participation is appropriately disclosed.

SECTION 9 - ACCEPTANCE PLAN

Inspection and acceptance is performed by the Contracting Officer's Representative (COR) on all data and non-data deliverables in accordance with the Quality Assurance Surveillance Plan (QASP)/QASP Matrix provided as Attachment 2.

SECTION 10 - INFORMATION ASSURANCE/INFORMATION SECURITY

The Contractor shall protect DoD sensitive unclassified data regardless of the location or ownership of the transport media, including, but not limited to mobile computing devices and removable storage media, whether Government furnished or contractor owned/leased. Contractor shall comply with all current information assurance and information security policies, procedures, and statutes applicable to DoD information technology, including the July 3, 2007 DoD CIO Policy Memorandum on Encryption of Sensitive Unclassified Data at Rest on Mobile Computing Devices and Removable Storage Media.

SECTION 11 – PRIVACY ACT COMPLIANCE

The contractor may be in contact with data and information subject to the Privacy Act of 1974 (Title 5 of the U.S. Code Section 552a). The contractor shall ensure that its employees assigned to this effort understand and adhere to the requirements of the Privacy Act and to Department of Defense and Department of the Navy regulations that implement the Privacy Act. Department of Navy policy and procedures implementing the Privacy Act are detailed in DoD Directive 5400.11 (DoD Privacy Program), available on-line at <http://www.dtic.mil/whs/directives/> and in SECNAVINST 5211.5E (Department of the Navy Privacy Act (PA) Program), which is available on-line at <http://privacy.navy.mil>. The contractor shall identify and safeguard data, information and reports accordingly. In addition, the contractor shall ensure that contractor employees assigned to the contract are trained on properly identifying and handling data and information subject to the Privacy Act prior to commencing work.

SECTION 12 – PROPRIETARY INFORMATION

No data provided to, or developed by, the contractor shall be used for any purpose other than the tasks assigned. All information (data files and hard copy) becomes the property of the Government and the contractor shall return them at the completion of the task. The Government shall not be required to pay royalties, recurring license fees, use tax or similar additional payments for any contractor-developed product or associated software presentation.

SECTION 13 - 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/TOM 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.

SECTION 14 - 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-85 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 text)

SECTION 15 - Enterprise Contractor Manpower Reporting Application (ECMRA)

The contractor shall report contractor labor hours (including subcontractor labor hours) required for performance of services provided under this contract 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) S, Utilities ONLY;
- (5) 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>.