

**PERFORMANCE WORK STATEMENT
NAVAL MEDICAL CENTER PORTSMOUTH COURIER SERVICES**

1.0 SCOPE

This is a non-personnel services contract to provide laboratory specimen courier services, hereinafter referred to as courier services, from the Naval Medical Center Portsmouth (NMCP) Branch Clinics and regional Tricare facilities listed in Attachment A to NMCP. The contractor shall provide all personnel, equipment, supplies, facilities, transportation, tools, materials, supervision, and other items and non-personal services necessary to perform courier services for laboratory specimens as defined in this Performance Work Statement. Laboratory specimens may be frozen, refrigerated or ambient and include blood, body fluid, tissue, swabs, and glass slides.

2.0 DESCRIPTION OF SERVICES

Contractor shall provide the safe transport between Government facilities listed in Attachment A of biomedical materials (patient specimens). This must include the proper receipt, distribution, storage and security of patient specimens in accordance with all federal* regulations governing the safe transport of these materials including, but not limited, to the following:

- Department of Transportation 49 CFR Parts 171-180 – Hazardous Materials: Infectious Substances; Harmonization with the United Nations Recommendations, Final Rule.
- Department of Labor/OSHA 29 CFR, Section 1910.1030-Bloodborne Pathogens
- Health Information Portability and Accountability Act (HIPAA) Privacy Rule 45 CFR Parts 160 1nd 164.

*** State and local regulations may be applicable if more stringent and do not conflict with the federal regulations.**

Attachment A provides the Courier Routes to include the facility name and location, frequency of pick up, times and days. In addition to these recurring routes, up to 5 STAT deliveries per month will be required. The STATs may require pick up from any of NMCP's nine (9) clinics, excluding Langley and Fort Eustis.

Contractor shall provide to each Government facility all materials necessary to comply with the logistics of a transportation program. This includes an adequate supply of materials necessary for the efficient, organized and coordinated receipt, transport, and delivery of specimens (e.g. securable multiple sized bags/containers, temperature condition stickers, labels, transportation receipt forms, rigid-sided containers, dry ice, coolers, rolling coolers, etc.).

Contractor shall provide transport vehicles that have all the necessary equipment to insure the integrity of ambient, refrigerated and frozen biomedical materials. All vehicles used in performance of the courier services must be licensed and meet the minimum requirements as mandated by the State of Virginia. Vehicles must provide protection for the items being transported to prevent exposure to the weather (direct sunlight, heat, rain, snow, water, etc.) and ensure items are secured to prevent theft or loss. All doors on the courier vehicle must be locked whenever the vehicle is left unattended. Any loss of a specimen is considered serious and potentially has a negative clinical impact. No item will be left unsecured for any reason.

Contractor must ensure transportation is provided in such a manner that the integrity and accountability of all items are maintained from contractor point of possession to the point of delivery to the Government. Government facilities will be responsible for processing and packaging all items in preparation for transportation, such that the transport device is tamper-proof and that Patient Identifiable Information (PII) is not visible to unauthorized personnel, including contractor courier(s). The Government will also provide a shipping manifest. The contractor shall provide onsite training to personnel located within the clinics and facilities on proper packaging and processing of specimens.

Contractor must have a state of the art, global tracking system that prevents any loss of transported items. This system must track and monitor specimen collection site and time of collection pick up and drop off at the various

government facilities. This system must be traceable and monitored for onsite delivery times and possible delays. Detailed data collection reports shall be made available to the Government via a web-based security portal. All electronic transmissions of data must meet all Federal, State and Local regulations, including data privacy in regards to HIPPA. Contractor shall educate all transport personnel on the policies and procedures for the receipt, tracking and delivery of the transported items.

3.0 QUALIFICATIONS & PERSONNEL

Contractor shall have at least one (1) year of experience in transporting biomedical materials and is responsible for obtaining all necessary licenses, permits, and/or certifications to provide the safe transportation of all items covered by this contract.

Personnel assigned by the contractor to perform the services covered by this contract shall be proficient in written and spoken English (38 USC 7402). Contractor representatives shall demonstrate appropriate professionalism/behavior, ethical behavior, and customer service in providing contracted courier services. In addition, the Contractor representative shall prominently display a contractor-issued identification badge.

Contractor shall ensure that all transport personnel are properly trained and that their competency is regularly assessed in the appropriate safety, packaging and environmental control procedures suitable to specimen type and distances transported. Critical elements of the training program will adhere to the regulations for the transport of bio-hazardous substances as cited in 49 CFR 172 Subpart H and must minimally include:

- a. Education on the types of biological materials transported including definitions of an infectious substance and a biological product.
- b. Education on appropriate hazardous material packaging and labeling.
- c. Requirements for the appropriate receipt of the packages including procedures for the completion and disposition of the shipping manifest.
- d. The use of appropriate containers to transport specimens between the origination point to the transport motor vehicle and, likewise, from the transport motor vehicle to the destination point.
- e. Appropriate installation, use and security of environmental temperature control devices that maintain ambient, refrigerated, frozen or incubated conditions in order to insure the integrity of the specimens and avoid loss or breakage of the containers.
- f. Identification of specimens requiring environmental temperature control storage.
- g. Certified education (hazmat training) on appropriate decontamination and notification procedures in case of accident or spills. This includes the identification and appropriate use of personal protective equipment and the use of mitigation and disinfection products.
- h. Education on procedures for hazardous spill communication, i.e. contact telephone numbers.
- i. Education on the protection of the privacy and confidentiality of the personally-identifiable information.

Base Access: Contractor shall obtain all local, State and Federal government licenses, passes and permits necessary to enter the government installation(s) to include motor vehicle registration and insurance, as required by the Government installation. Commander, Navy Installations Command (CNIC), has established the Navy Commercial Access Control System (NCACS), a standardized process for granting unescorted access privileges to vendors, contractors, suppliers and service providers not otherwise entitled to the issuance of a Common Access Card (CAC) who seek access to and can provide justification to enter Navy installations and facilities. *Vendors visiting Naval Medical Center Portsmouth (NMCP) may obtain daily passes directly from Naval Station Norfolk (NSN) Pass and ID office, located at NSN (Bldg CD-9), 9040*

Hampton Blvd, Norfolk, Virginia, 23505, by submitting identification credentials for verification and undergoing a criminal screening/ background check. Alternatively, if the vendor so chooses, it may voluntarily elect to obtain long-term credentials through enrollment, registration, background vetting, screening, issuance of credentials, and electronic validation of credentials at its own cost through one of the designated independent contractor NCACS service providers. Credentials will be issued every five years and access privileges will be reviewed / renewed on an annual basis. The costs incurred to obtain Navy installation access of any kind are not reimbursable, and the price(s) paid for obtaining long-term NCACS credentials will not be approved as a direct cost of this contract. Further information regarding NCACS can be found at http://cnic.navy.mil/CNIC_HQ_Site/index.htm.

Any new requirements for mandatory education and/or competency reassessment, which occur during contract performance, must be completed by the individual contractor employee(s) within established timeframes.

4.0 QUALITY CONTROL

Quality Control (QC) Plan: The contractor shall develop and maintain an effective QC plan to ensure services are performed in accordance with this PWS. The contractor shall develop and implement procedures to identify, prevent, remedy and ensure non-recurrence of defective services. The contractor shall provide a method to accept and resolve customer complaints and notify the customer and COR of the resolution. The contractor shall immediately notify the COR upon receipt of a customer complaint so that joint validation may be accomplished. A copy of the QC Plan shall be provided to the COR within 10 days of contract award.

Contractor shall have a contingency system in place to ensure 100% courier route performance. Contractor shall provide an emergency contact person (other than the courier-employee) to immediately address inter-route issues that occur. This contact must be available for emergency response within the timeframes covered in the courier route plan (Attachment A) and throughout extended time periods when the courier is not able to meet the stated delivery times. In addition, this contact must have the capability to be in immediate communication with the courier employee performing the services in cases of emergency or to determine location. The contact information, i.e. name(s) and/or office(s) and telephone number(s), for these emergency contact personnel shall be made available after award.

Contractor shall designate a coordinator to organize activities, monitor services, and respond to customer service problems. Coordinator shall be able to provide oversight of overall and day to day coordination of the courier schedule to include dispatch, timeliness, and communication.

Quality Assurance: The government shall evaluate the contractor's performance under this contract in accordance with the Quality Assurance Surveillance Plan (QASP). This plan is primarily focused on what the Government must do to ensure that the contractor has performed in accordance with the performance standards. It defines how the performance standards will be applied, the frequency of surveillance, and the minimum acceptable defect rate(s).

5.0 PRIVACY AND SECURITY OF PROTECTED HEALTH INFORMATION

Introduction

In accordance with DoD 6025.18-R "Department of Defense Health Information Privacy Regulation," January 24, 2003, the Business Associate meets the definition of Business Associate. Therefore, a Business Associate Agreement is required to comply with both the Health Insurance Portability and Accountability Act (HIPAA) Privacy and Security regulations. This clause serves as that agreement whereby the Business Associate agrees to abide by all applicable HIPAA Privacy and Security requirements regarding health information as defined in this clause, and in DoD 6025.18-R and DoD 8580.02-R, as amended. Additional requirements will be addressed when implemented.

a. Definitions. As used in this clause generally refer to the Code of Federal Regulations (CFR) definition unless a more specific provision exists in DoD 6025.18-R or DoD 8580.02-R.

(1) *HITECH Act* shall mean the Health Information Technology for Economic and Clinical Health Act included in the American Recovery and Reinvestment Act of 2009.

(2) *Individual* has the same meaning as the term “individual” in 45 CFR [160.103](#) and shall include a person who qualifies as a personal representative in accordance with 45 CFR 164.502(g).

(3) Privacy Rule means the Standards for Privacy of Individually Identifiable Health Information at 45 CFR part 160 and part 164, subparts A and E.

(4) Protected Health Information has the same meaning as the term “protected health information” in 45 CFR [160.103](#), limited to the information created or received by the Business Associate from or on behalf of the Government pursuant to the Contract.

(5) Electronic Protected Health Information has the same meaning as the term “electronic protected health information” in 45 CFR 160.103.

(6) Required by Law has the same meaning as the term “required by law” in 45 CFR 164.103.

(7) Secretary means the Secretary of the Department of Health and Human Services or his/her designee.

(8) Security Incident will have the same meaning as the term “security incident” in 45 CFR 164.304, limited to the information created or received by Business Associate from or on behalf of Covered Entity.

(9) Security Rule means the Health Insurance Reform: Security Standards at 45 CFR part 160, 162 and part 164, subpart C.

(10) Terms used, but not otherwise defined, in this Clause shall have the same meaning as those terms in 45 CFR 160.103, 160.502, 164.103, 164.304, and 164.501.

b. The Business Associate shall not use or further disclose Protected Health Information other than as permitted or required by the Contract or as Required by Law.

c. The Business Associate shall use appropriate safeguards to maintain the privacy of the Protected Health Information and to prevent use or disclosure of the Protected Health Information other than as provided for by this Contract.

d. The HIPAA Security administrative, physical, and technical safeguards in 45 CFR 164.308, 164.310, and 164.312, and the requirements for policies and procedures and documentation in 45 CFR 164.316 shall apply to Business Associate. The additional requirements of Title XIII of the HITECH Act that relate to the security and that are made applicable with respect to covered entities shall also be applicable to Business Associate. [The Business Associate agrees to use administrative, physical, and technical safeguards that reasonably and appropriately protect the confidentiality, integrity, and availability of the electronic protected health information that it creates, receives, maintains, or transmits in the execution of this Contract.](#)

e. The Business Associate shall, at their own expense, take action to mitigate, to the extent practicable, any harmful effect that is known to the Business Associate of a use or disclosure of Protected Health Information by the Business Associate in violation of the requirements of this Clause. These mitigation actions will include as a minimum those listed in the TMA Breach Notification Standard Operating Procedure (SOP), which is available at: <http://www.tricare.mil/tmaprivacy/breach.cfm>

f. The Business Associate shall report to the Government any security incident involving protected health information of which it becomes aware.

g. The Business Associate shall report to the Government any use or disclosure of the Protected Health Information not provided for by this Contract of which the Business Associate becomes aware.

h. The Business Associate shall ensure that any agent, including a sub Business Associate, to whom it provides Protected Health Information received from, or created or received by the Business Associate, on behalf of the Government, agrees to the same restrictions and conditions that apply through this Contract to the Business Associate with respect to such information.

i. The Business Associate shall ensure that any agent, including a subBusiness Associate, to whom it provides electronic Protected Health Information, agrees to implement reasonable and appropriate safeguards to protect it.

j. The Business Associate shall provide access, at the request of the Government, and in the time and manner [reasonably](#) designated by the Government to Protected Health Information in a Designated Record Set, to the Government or, as directed by the Government, to an Individual in order to meet the requirements under 45 CFR 164.524.

k. The Business Associate shall make any amendment(s) to Protected Health Information in a Designated Record Set that the Government directs or agrees to pursuant to 45 CFR 164.526 at the request of the Government, and in the time and manner [reasonably](#) designated by the Government.

l. The Business Associate shall make internal practices, books, and records relating to the use and disclosure of Protected Health Information received from, or created or received by the Business Associate, on behalf of the Government, available to the Government, or at the request of the Government to the Secretary, in a time and manner [reasonably](#) designated by the Government or the Secretary, for purposes of the Secretary determining the Government's compliance with the Privacy Rule.

m. The Business Associate shall document such disclosures of Protected Health Information and information related to such disclosures as would be required for the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

n. The Business Associate shall provide to the Government or an Individual, in time and manner [reasonably](#) designated by the Government, information collected in accordance with this Clause of the Contract, to permit the Government to respond to a request by an Individual for an accounting of disclosures of Protected Health Information in accordance with 45 CFR 164.528.

General Use and Disclosure Provisions

Except as otherwise limited in this Clause, the Business Associate may use or disclose Protected Health Information on behalf of, or to provide services to, the Government for treatment, payment, or healthcare operations purposes, in accordance with the specific use and disclosure provisions below, if such use or disclosure of Protected Health Information would not violate the HIPAA Privacy Rule, the HIPAA Security Rule, DoD 6025.18-R or DoD 8580.02-R if done by the Government. The additional requirements of Title XIII of the HITECH Act that relate to privacy and that are made applicable with respect to covered entities shall also be applicable to Business Associate.

Specific Use and Disclosure Provisions

a. Except as otherwise limited in this Clause, the Business Associate may use Protected Health Information for the proper management and administration of the Business Associate or to carry out the legal responsibilities of the Business Associate.

b. Except as otherwise limited in this Clause, the Business Associate may disclose Protected Health Information for the proper management and administration of the Business Associate, provided that disclosures are required by law, or the Business Associate obtains reasonable assurances from the person to whom the information is disclosed that it will remain confidential and used or further disclosed only as required by law or for the purpose for which it was disclosed to the person, and the person notifies the Business Associate of any instances of which it is aware in which the confidentiality of the information has been breached.

c. Except as otherwise limited in this Clause, the Business Associate may use Protected Health Information to provide Data Aggregation services to the Government as permitted by 45 CFR 164.504(e)(2)(i)(B).

d. Business Associate may use Protected Health Information to report violations of law to appropriate Federal and State authorities, consistent with 45 CFR 164.502(j)(1).

Obligations of the Government

Provisions for the Government to Inform the Business Associate of Privacy Practices and Restrictions

a. [The](#) Government shall provide the Business Associate with the notice of privacy practices that the Government produces in accordance with 45 CFR 164.520.

b. The Government shall provide the Business Associate with any changes in, or revocation of, permission by Individual to use or disclose Protected Health Information, if such changes affect the Business Associate's permitted or required uses and disclosures.

c. The Government shall notify the Business Associate of any restriction to the use or disclosure of Protected Health Information that the Government has agreed to in accordance with 45 CFR 164.522.

Permissible Requests by the Government

The Government shall not request the Business Associate to use or disclose Protected Health Information in any manner that would not be permissible under the HIPAA Privacy Rule, [the HIPAA Security Rule, or any applicable Government regulations \(including without limitation, DoD 6025.18-R and DoD 8580.02-R\)](#) if done by the Government, except for providing Data Aggregation services to the Government and for management and administrative activities of the Business Associate as otherwise permitted by this clause.

Termination

a. Termination. A breach by the Business Associate of this clause, may subject the Business Associate to termination under any applicable default or termination provision of this Contract.

b. Effect of Termination.

(1) If this contract has records management requirements, the records subject to the Clause should be handled in accordance with the records management requirements. If this contract does not have records management requirements, the records should be handled in accordance with paragraphs (2) and (3) below

(2) If this contract does not have records management requirements, except as provided in paragraph (3) of this section, upon termination of this Contract, for any reason, the Business Associate shall return or destroy all Protected Health Information received from the Government, or created or received by the Business Associate on behalf of the Government. This provision shall apply to Protected Health Information that agents of the Business Associate may come in contact. The Business Associate shall retain no copies of the Protected Health Information.

(3) If this contract does not have records management provisions and the Business Associate determines that returning or destroying the Protected Health Information is infeasible, the Business Associate shall provide to the Government notification of the conditions that make return or destruction infeasible. Upon mutual agreement of the Government and the Business Associate that return or destruction of Protected

Health Information is infeasible, the Business Associate shall extend the protections of this Contract to such Protected Health Information and limit further uses and disclosures of such Protected Health Information to those purposes that make the return or destruction infeasible, for so long as the Business Associate maintains such Protected Health Information.

Miscellaneous

a. Regulatory References. A reference in this Clause to a section in DoD 6025.18-R, DoD 8580.02-R, Privacy Rule or Security Rule means the section currently in effect or as amended, and for which compliance is required.

b. Survival. The respective rights and obligations of Business Associate under the “Effect of Termination” provision of this Clause shall survive the termination of this Contract.

c. Interpretation. Any ambiguity in this Clause shall be resolved in favor of a meaning that permits the Government to comply with DoD 6025.18-R, DoD 8580.02-R, the HIPAA Privacy Rule or the HIPAA Security Rule.

6.0 SECURITY

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-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.

In order to maintain access to required systems, the contractor shall ensure completion of annual Information Assurance (IA) training, monitor expiration of requisite background investigations, and initiate reinvestigations as required.

7.0 DELIVERABLES

Monthly Status Report: The contractor shall develop and submit a monthly status report on company letterhead and submitted not later than the tenth (10th) day of the month. This status report shall provide a synopsis of any issues and/or concerns, list of missed and/or late routes and the reasons, and any other information that the contractor determines is necessary/relevant. Additionally, updates on any qualifications on contract employees will also be provided in the Monthly Status Report.

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 NAVSUP WSS Security Management System 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>.

ATTACHMENT A: The routes to include pick up and drop off locations, times, days and frequency are:

ROUTE 1. MONDAY thru FRIDAY

Pick-Up From:

USAF Hospital Langley AFB / 77 Nealy Ave / Hampton VA 23665

Mon-Fri / 0845 1st Pickup

Mon-Fri / 1400 2nd Pickup

McDonald Army Health Clinic / 576 Jefferson Ave / Fort Eustis VA 23604

Mon-Fri / 0915 1st Pickup

Mon-Fri / 1430 2nd Pickup

Yorktown Naval Weapons Station / 160 Main Rd Suite 90 / Yorktown VA 23619

Mon-Fri / 0930 1st Pickup

Mon-Fri / 1500 2nd Pickup

Boone Clinic / 1035 Nider Blvd Suite 100 / Virginia Beach VA 23459

Mon-Fri / 1030 1st Pickup

Mon-Fri / 1615 2nd Pickup

Sewells Point Clinic / 1721 Taussig Blvd / Norfolk VA 23505

Mon-Fri / 1100 1st Pickup

Mon-Fri / 1645 2nd Pickup

Delivery To:

Naval Medical Center Portsmouth (NMCP) Laboratory / 620 John Paul Jones Circle / Portsmouth VA 23708

Mon-Fri / 1130 1st Delivery

Mon-Fri / 1715 2nd Delivery

ROUTE 2. MONDAY thru FRIDAY

Pick-Up From:

Northwest Clinic / 1317 Ballahack Rd / Chesapeake VA 23322

Mon-Fri / 1000 1st Pickup

Mon-Fri / 1530 2nd Pickup

TPC Chesapeake / 1011 Eden Way N Suite H / Chesapeake VA 23320

Mon-Fri / 1030 1st Pickup

Mon-Fri / 1545 2nd Pickup

Delivery To:

Naval Medical Center Portsmouth (NMCP) Laboratory / 620 John Paul Jones Circle / Portsmouth VA 23708

Mon-Fri / 1100 1st Delivery

Mon-Fri / 1630 2nd Delivery

ROUTE 3. MONDAY thru FRIDAY

Pick-Up From:

Dam Neck Clinic / 1885 Terrier Avenue / Virginia Beach VA 23461

Mon-Fri / 1000 1st Pickup

Mon-Fri / 1515 2nd Pickup

Oceana Clinic / 1550 Tomcat Blvd / Virginia Beach VA 23460

Mon-Fri / 1015 1st Pickup

Mon-Fri / 1530 2nd Pickup

TPC VA Beach / 2100 Lynnhaven Parkway / Virginia Beach VA 23456
Mon-Fri / 1045 1st Pickup
Mon-Fri / 1600 2nd Pickup

Delivery To:

Naval Medical Center Portsmouth (NMCP) Laboratory / 620 John Paul Jones Circle / Portsmouth VA 23708
Mon-Fri / 1115 1st Delivery
Mon-Fri / 1630 2nd Delivery

LATE WEEK DAY ROUTE 1. MONDAY thru FRIDAY

Pick-Up From:

Oceana / 1550 Tomcat Blvd / Virginia Beach VA 23460
Mon-Fri / 1830

Boone Clinic / 1035 Nider Blvd Suite 100 / Virginia Beach VA 23459

Mon-Fri / 1900

Delivery To:

Naval Medical Center Portsmouth (NMCP) Laboratory / 620 John Paul Jones Circle / Portsmouth VA 23708
Mon-Fri / 1930

LATE WEEK DAY ROUTE 2. MONDAY thru FRIDAY

Pick-Up From:

TPC VA Beach / 2100 Lynnhaven Parkway / Virginia Beach VA 23456
Mon-Fri / 1830

TPC Chesapeake / 1011 Eden Way N Suite H / Chesapeake VA 23320

Mon-Fri / 1900

Delivery To:

Naval Medical Center Portsmouth (NMCP) Laboratory / 620 John Paul Jones Circle / Portsmouth VA 23708
Mon-Fri / 1930

WEEKEND ROUTE. SUNDAY and SATURDAY

Pick-Up From:

Boone Clinic / 1035 Nider Blvd Suite 100 / Virginia Beach VA 23459

Sun & Sat / 1430

TPC VA Beach / 2100 Lynnhaven Parkway / Virginia Beach VA / 23456

Sun & Sat / 1500

TPC Chesapeake / 1011 Eden Way N Suite H / Chesapeake VA 23320

Sun & Sat / 1530

Delivery To:

Naval Medical Center Portsmouth (NMCP) Laboratory / 620 John Paul Jones Circle / Portsmouth VA 23708
Sun & Sat / 1600

NOTE: Courier services are not required on Federal Holidays. The 10 holidays observed by the Federal Government are: New Year's Day (January 1st), Martin Luther King's Birthday (3rd Monday in January), Presidents' Day (3rd Monday in February), Memorial Day (last Monday in May), Independence Day (July 4th), Labor Day (1st Monday in September), Columbus Day (2nd Monday in October), Veterans Day (November 11), Thanksgiving Day

(4th Thursday in November), Christmas Day (December 25th) and any other day specifically declared by the President of the United States to be a national holiday.

When one of the above designated legal holidays falls on a Sunday, the following Monday will be observed as a legal holiday. When a legal holiday falls on a Saturday, the preceding Friday is observed as a holiday by U.S. Government agencies.