

**STATEMENT OF WORK FOR THE LEASING OF PROPANE TANKS AND BULK PROPANE
DELIVERY TO FORT PICKETT IN SUPPORT OF NAVAL FACILITIES ENGINEERING COMMAND
(NAVFAC) MID-ATLANTIC**

1.0. Introduction

This requirement is for the leasing of propane tanks and acquisition and delivery of propane to Fort Pickett, Virginia in support of Naval Facilities Engineering Command (NAVFAC) Mid-Atlantic. The US Navy utilizes the above buildings on Fort Pickett for training and ordnance testing. The Contractor shall provide all labor, equipment, material, supervision, and transportation necessary to supply and deliver approximately 24,000 gallons of propane gas annually for the following buildings:

Bldg. 1358 – 1,000 Gallon Tank
Bldg. 1365 – 1,000 Gallon Tank
Bldg. 1367 – 1,000 Gallon Tank
Bldg. 1386 – 500 Gallon Tank
Bldg. 1718 – 1,000 Gallon Tank
Bldg. 1724 – 1,000 Gallon Tank
Bldg. 1725 – 1,000 Gallon Tank
Bldg. 1726 – 1,000 Gallon Tank
Bldg. 1727 – 1,000 Gallon Tank

2.0. General Information

The Government intends on issuing a Firm Fixed Price (FFP), Small Business (SB) Set-aside delivery order with a twelve month base year plus two (2) twelve month option years. The ordering season begins on 01 September through 31 May annually. The boilers are generally shut off during the summer season as they are not in use; therefore, no propane will be used during the summer months.

Period of Performance	
Base Year	12 January 2023 through 11 January 2024
Option I	12 January 2024 through 11 January 2025
Option II	12 January 2025 through 11 January 2026

3.0. Requirements/Scope

- 3.1. The Contractor shall provide eight (8) 1,000 gallon propane tanks and one (1) 500 gallon propane tank to be installed on government furnished concrete slabs at Fort Pickett, Virginia, for the entire period of performance.
- 3.2. The Contractor shall check the level of propane in ALL tanks every MONTH.
- 3.3. The Contractor shall fill the propane tanks to capacity, if required, every month. Tanks shall not go below the "Critical Low Point" of 20% of the capacity of the tank. If any of the tanks falls to this level the contractor shall refill the tanks as needed.
- 3.4. The Government will inform the Contractor if propane will be needed more frequently than every month.
- 3.5. The tanks, installation and hardware shall include the necessary piping, regulators and other related equipment to connect the tanks to the government piping already existing at the location.
- 3.6. The tanks will be installed on Government Property however the Contractor shall retain ownership throughout the life of the delivery order.
- 3.7. Pricing for this requirement shall be total cost per gallon, which shall include all applicable Delivery, Admin, Environmental, Tank Change Out, Fuel Surcharges, Federal, State and Local Taxes, Other Fees and Surcharges.

4.0. Special Requirements

- 4.1. The Contractor shall interface with designated points of contact (POC) that will receive and process the site's delivery tickets and supply Base Access Badges.
- 4.2. The Contractor shall obtain Defense Biometrics Identification System (DBIDS) Passes for employees that will be accessing the base.
- 4.3. The Contractor shall supply an annual economic cost adjustment factor to be utilized to adjust the contract costs according to Market fluctuations. This should be submitted as total cost per gallon. Cost adjustments will be capped at plus or minus 10% of the current market price.
- 4.4. The Contractor shall be able to accept modifications to the delivery order to add or delete accounts as necessary.
- 4.5. Contractor shall possess and maintain Federal, State, National, and, Local permits needed to transport material on and off the base as necessary.
- 4.6. Leased Tanks – The Contractor has 30 days from the start of the period of performance to replace eight (8) 1,000 gallon tanks and one (1) 500 gallon tank. The Contractor shall provide industry standard tanks in compliance with Federal, State, National and Local codes, standards and regulations governing services.
- 4.7. Government Owned Tanks (if applicable) – The Contractor shall provide all tank inspections to maintain compliance with all Federal, State, National and Local codes, standards, and regulations.
- 4.8. Contractor shall respond within an 8 hour timeframe for all urgent deliveries.

5.0. Invoicing

Invoices shall be submitted on a monthly basis only for the amount of propane actually delivered. All invoices shall be submitted to the following address for payment:

Utility Invoice Processing Center
(Insert respective Government Account Number)
Box 159
9226 Third Avenue
Norfolk VA 23511-2313

6.0. Deliverables

- 6.1. The Government requires HD5 consumer grade propane with the following specifications:
 - 6.1.1. Minimum of 90% propane
 - 6.1.2. Maximum of 5% propylene
 - 6.1.3. Other gases may constitute the remainder (iso-butane, butane, methane, etc.)
- 6.2. The HD5 specification is based on "allowable" contents. For instance, 99% propane and 1% propylene is HD5 grade propane the same as 95% propane and 5% propylene is HD5 propane.

Note: Although the product consistency and purity is different, both mixtures are considered HD5 because they fall within the allowable limits for the product to be named and labeled as such.

7.0. Security Requirements

All work identified by this PWS is unclassified in nature and a security clearance is not required. However, any contract employee assigned to this contract must be a U.S. citizen. The Contractor shall comply with all applicable Department of Defense (DOD) and Department of the Navy (DON) physical security regulations and procedures during the performance of this contract. Contractors shall not disclose and must safeguard procurement sensitive

information, computer systems, privacy act data, ship movement schedules, and Government personnel work products that are obtained or generated in the performance of this contract.

8.0. Personnel Compliance

The Contractor shall ensure that contractor personnel observe and comply with all local and higher authority policies, regulations, and procedures concerning fire, safety, environmental protection, sanitation, security, traffic, parking, energy conservation, flag courtesy, "off limits" areas, and possession of firearms or other lethal weapons. When two or more directives or instructions apply, the contractor shall comply with the more stringent of the policies.

9.0. Contractor Responsibility

The contractor shall comply with all security requirements in accordance with the directives and site specific regulations. The Government reserves the right to grant and revoke access for particular individual(s) to its facilities. This will not constitute a breach of contract or change to the PWS. For the purposes of this PWS, the term "Contractor Employee" applies to all Contractor employees and sub-contractor employees performing work under this PWS and resultant contract.

10.0. CONTRACTOR UNCLASSIFIED ACCESS TO FEDERALLY CONTROLLED FACILITIES, SENSITIVE INFORMATION, INFORMATION TECHNOLOGY (IT) SYSTEMS OR PROTECTED HEALTH INFORMATION

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 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 Command's Security Manager upon arrival to the 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) or T5 or T5R equivalent investigation, which is a higher level investigation than the National Agency Check with Law and Credit (NACLC)/T3/T3R described below. Due to the

privileged system access, an investigation suitable for High Risk national security 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 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 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 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 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

Security policy requires that all positions be given a sensitivity value based on level of risk factors to ensure appropriate protective measures are applied. Contractor employees under this contract are recognized as Non-Critical Sensitive [ADP/IT-II] positions 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 as National Security Positions. At a minimum, each contractor employee must be a US citizen and have a favorably completed NACLC or T3 or T3R equivalent investigation to obtain a favorable determination for assignment to a non-critical sensitive or IT-II position. The investigation 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 Command's Security Manager upon arrival to the 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 Command's Information Assurance Manager. Completion and approval of a System Authorization Access Request Navy (SAAR-N) form is required for all individuals accessing Information Technology resources. The SAAR-N shall be forwarded to the 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 Command Security Manager. The Command's Security Manager will review the submitted documentation for completeness prior to submitting it to the Office of Personnel Management (OPM); Potential suitability or security issues identified may render the contractor employee ineligible for the assignment. An unfavorable determination 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 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 DOD 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 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) or T1 investigation equivalent 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 T1 investigation equivalent, 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.