STATEMENT OF WORK
FOR
HELIUM TUBE TRALIERS

1.0 SCOPE

The Naval Surface Warfare Center, Panama City Division, FL, (NSWC PCD) has a requirement for the delivery of helium tube trailers.

2.0 APPLICABLE DOCUMENTS

The following documents, of the exact issue shown, form a part of this SOW to the extent specified herein. In the event of conflict between the documents referenced herein and the SOW, the contents of this SOW shall take precedence.

2.1 Military Standards:

- None.

2.2 Military Specifications:

- None.

2.3 Other Documents:

- None.

3.0 REQUIREMENTS

The Contractor shall deliver the following within 2 weeks of award of contract.

Qty.: 750 CCF
Item: Helium MIL SPEC SIZE TUBE TRAILER, MIL SPEC PRF 27407D, Grade B

Delivered to NSWC PCD.

4.0 GOVERNMENT FURNISHED PROPERTY (GFP): None

4.1 Access to Government Facilities

The Government will provide the contractor access to Government facilities to accomplish statement of work tasking. The Contractor shall provide a list of employees who require access to these areas, including standard security clearance information for each person, to the Procuring Contracting Officer (PCO) no later than three business days after the date of award. Access to Government buildings at Naval Support Activity Panama City (NSA PC) is from 0600 to 1800 Monday through Friday, except Federal holidays. Normal work hours are from 0700 to 1700, Monday through Friday. Contractor employees shall be under Government oversight at all times. Government oversight requires that a Government employee be present in the same building/facility whenever Contractor employee(s) are performing work under this task order. Contractor personnel are not allowed to access any Government buildings at NSA PC outside the hours of 0600 to 1800 without the express approval of the Procuring Contracting Officer (PCO). When a Government facility is closed or early dismissal of Federal employees is directed due to severe weather, security threat, or a facility related problem that prevents personnel from working, onsite Contractor personnel regularly assigned to work at that facility should follow the same reporting and departure directions given to Government personnel.

5.0 DATA DELIVERABLES

Data shall be provided in accordance with the Contract Data Requirements List (CDRL) DD Form 1423.

6.0 PERIOD OF PERFORMANCE

The Contractor shall deliver within 2 weeks of award.

7.0 SECURITY

This requirement is UNCLASSIFIED. The Contractor will not require access to nor be required to generate classified information to perform the requirement.

7.1 RELEASE OF INFORMATION

(a) Release of information shall be in accordance with Section I, DFARS Clause 252.204-7000, Disclosure of Information.

(b) All technical data provided to the contractor by the Government shall be protected from public disclosure in accordance with the markings contained thereon. All other information relating to the items to be delivered or services to be performed under this task order may not be disclosed by any means without prior approval of the appropriate NSWC PCD authority. Dissemination or public disclosure includes, but is not limited to, permitting access to such information by foreign nationals or by any other person or entity; publication of technical or scientific papers; advertising; or any other proposed public release. The contractor shall provide adequate physical protection to such information to preclude access by any person or entity not authorized such access by the Government.

7.2 Controlled Unclassified Information (CUI)

Controlled unclassified information (CUI) is official information that requires the application of controls and protective measures for a variety of reasons and has not been approved for public release, to include technical information, proprietary data, information requiring protection under the Privacy Act of 1974, and Government-developed privileged information involving the award of contracts. CUI is a categorical designation that refers to unclassified information that does not meet the standards for National Security Classification under Executive Order 13526, but is (a) pertinent to the national interest of the United States or to the important interests of entities outside the Federal Government, and (b) under law or policy requires protection from unauthorized disclosure, special handling safeguards, or prescribed limits on exchange or dissemination.

7.3 Minimum Requirements for Access to Controlled Unclassified Information (CUI)

Access to CUI, user level access to DON or DoD networks and information systems, system security and network defense systems, and to system resources providing visual access and/or ability to input, delete or otherwise manipulate sensitive information without controls to identify and deny sensitive information, requires security clearance eligibility, based on a Tier 3 Background Investigation, and a favorable adjudication by the Defense Counterintelligence and Security Agency, Consolidated Adjudications (DCSA CAS), or Interim/Temporary access to CUI based on a determination by the NSWC PCD Security Manager based on a favorable review of an individuals completed Electronic Questionnaire for Investigation Processing (SF 86), and favorable FBI fingerprint results. Contact NSWC PCD Personnel Security for initiation of the SF86 and FBI fingerprinting, the CUI determination, and validation that employees have the required eligibility, prior to providing access to CUI.

7.4 Minimum Protection Requirements for Controlled Unclassified Information

Security classification guides and unclassified limited documents (e.g., CUI, Distribution Statement

Controlled) are not authorized for public release and, therefore, cannot be posted on a publicly accessible webserver or transmitted over the Internet unless appropriately encrypted.

7.5 CUI

CUI is a designation, not a classification. CUI is used by Department of Defense (DoD) and a number of other federal agencies to identify information or material, which although unclassified, disclosure to the public of the information would reasonably be expected to cause a foreseeable harm to an interest protected by one or more provisions of the FOIA. This includes information that qualifies for protection pursuant to the provisions of the Privacy Act of 1974, as amended. CUI must be marked, controlled and safeguarded in accordance with DoDI 5200.48, DoD Information Security Program: Controlled Unclassified Information (CUI).

7.6 Security of Unclassified DoD Information on Non-DoD Information Systems (DoDI 8582.01)

7.6.1 **DoD Policy**

Adequate security shall be provided for all unclassified DoD information on non-DoD information systems. Appropriate requirements shall be incorporated into all contracts, grants, and other legal agreements with non-DoD entities.

Information Safeguards are applicable to unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems, to the extent provided by the applicable contract, grant, or other legal agreement with the DoD.

7.6.2 Information Safeguards

Unclassified DoD information that has not been cleared for public release may be disseminated by the Contractor, grantee, or awardee to the extent required to further the contract, grant, or agreement objectives, provided that the information is disseminated within the scope of assigned duties and with a clear expectation that confidentiality will be preserved. Examples include:

(a) Non-public information provided to a Contractor (e.g., with a request for proposal).

(b) Information developed during the course of a contract, grant, or other legal agreement (e.g., draft documents, reports, or briefings and deliverables).

(c) Privileged information contained in transactions (e.g., privileged contract information, program schedules, contract-related event tracking).

Note: It is recognized that adequate security will vary depending on the nature and sensitivity of the information on any given non-DoD information system. However, all unclassified DoD information in the possession or control of non-DoD entities on non-DoD information systems shall minimally be safeguarded as follows:

(a) Do not process unclassified DoD information on publically available computers (e.g., those available for use by the general public in kiosks or hotel business centers).

(b) Protect unclassified DoD information by at least one physical or electronic barrier (e.g., locked container or room, logical authentication or logon procedure) when not under direct individual control of an authorized user.

(c) At a minimum, overwrite media that have been used to process unclassified DoD information before external release or disposal.

(d) Encrypt all information that has been identified as CUI when it is stored on mobile computing devices such as laptops and personal digital assistants, compact disks, or authorized removable storage media such as thumb drives and compact disks, using the best encryption technology available to the Contractor or teaming partner.

(e) Limit transfer of unclassified DoD information to subcontractors or teaming partners with a need to know and obtain a commitment from them to protect the information they receive to at least the same level of protection as that specified in the contract or other written agreement.

(f) Transmit e-mail, text messages, and similar communications containing unclassified DoD information using technology and processes that provide the best level of privacy available, given facilities, conditions, and environment. Examples of recommended technologies or processes include closed networks, virtual private networks, public key-enabled encryption, and transport layer security (TLS).

(g) Encrypt organizational wireless connections and use encrypted wireless connections where available when traveling. If encrypted wireless is not available, encrypt document files (e.g., spreadsheet and word processing files), using at least application-provided password protected level encryption.

(h) Transmit voice and fax transmissions only when there is a reasonable assurance that access is limited to authorized recipients.

(i) Do not post unclassified DoD information to website pages that are publicly available or have access limited only by domain or Internet protocol restriction. Such information may be posted to website pages that control access by user identification and password, user certificates, or other technical means and provide protection via use of transport layer security or other equivalent technologies during transmission. Access control may be provided by the intranet (vice the website itself or the application it hosts).

(j) Provide protection against computer network intrusions and data exfiltration, minimally including:

(1) Current and regularly updated malware protection services, e.g., anti-virus, anti-spyware.

(2) Monitoring and control of both inbound and outbound network traffic (e.g., at the external boundary, sub-networks, individual hosts), including blocking unauthorized ingress, egress, and exfiltration through technologies such as firewalls and router policies, intrusion prevention or detection services, and host-based security services.

(3) Prompt application of security-relevant software patches, service packs, and hot fixes.

(k) Comply with other current Federal and DoD information protection and reporting requirements for specified categories of information (e.g., medical, proprietary, Critical Program Information (CPI), personally identifiable information, export controlled) as specified in contracts, grants, and other legal agreements.

(l) Report loss or unauthorized disclosure of unclassified DoD information in accordance with contract, grant, or other legal agreement requirements and mechanisms.

(m) Do not use external IT services (e.g., e-mail, content hosting, database, document processing) unless they provide at least the same level of protection as that specified in the contract or other written agreement.

7.7 Operations Security (OPSEC)

Operations Security (OPSEC) is concerned with the protection of critical information: facts about intentions, capabilities, operations, or activities that are needed by adversaries or competitors to bring about failure or unacceptable consequences of mission accomplishment.

Critical information includes information regarding:

- Operations, missions, and exercises, test schedules or locations;
- Location/movement of sensitive information, equipment, or facilities;
- Force structure and readiness (e.g., recall rosters);
- Capabilities, vulnerabilities, limitations, security weaknesses;
- Intrusions/attacks of DoD networks or information systems;
- Network (and system) user identifications and passwords;
- Movements of key personnel or visitors (itineraries, agendas, etc.); and
- Security classification of equipment, systems, operations, etc.

The Contractor, subcontractors and their personnel shall employ the following countermeasures to mitigate the susceptibility of critical information to exploitation, when applicable:

- Practice OPSEC and facilitate OPSEC awareness;
- Immediately retrieve documents from printers assessable by the public;
- Shred sensitive and Controlled Unclassified Information (CUI) documents when no longer needed;
- Protect information from personnel without a need-to-know;
- When promulgating information, limit details to that essential for legitimacy;
- During testing and evaluation, practice OPSEC methodologies of staging out of sight, desensitization, or speed of execution, whenever possible.

8.0 DISTRIBUTION LIMITATION STATEMENTS

Distribution Statements and Warning Notices: *The Contractor shall place the appropriate Distribution Statement on information associated/generated with this contractual effort, per the applicable Security Classification Guide, and carry forward the markings on documents provided by the government, along with the following statements on all technical documents/media, as applicable.*

WARNING - THIS DOCUMENT CONTAINS TECHNICAL DATA WHOSE EXPORT IS RESTRICTED BY THE ARMS EXPORT CONTROL ACT (SECTION 2751 OF TITLE 22, UNITED STATES CODE) OR THE EXPORT CONTROL REFORM ACT OF 2018 (CHAPTER 58 SECTIONS 4801-4852 OF TITLE 50, UNITED STATES CODE). VIOLATIONS OF THESE EXPORT LAWS ARE SUBJECT TO SEVERE CRIMINAL PENALTIES. DISSEMINATE IN ACCORDANCE WITH PROVISIONS OF DOD DIRECTIVE 5230.25 AND DOD INSTRUCTION 2040.02.

DESTRUCTION NOTICE - CLASSIFIED INFORMATION, DESTROY IN ACCORDANCE WITH SECNAVINST 5510.36, (DON INFORMATION SECURITY PROGRAM) OR NISPOM RULE. UNCLASSIFIED LIMITED DOCUMENTS, (E.G., CUI, DISTRIBUTION STATEMENT CONTROL) DESTROY PER DODI 5200.48.