STATEMENT OF WORK
FOR
THERMAL EQUIPMENT RENTAL TO SUPPORT SYSTEM TESTING

1.0 SCOPE

The Naval Surface Warfare Center Panama City Division (NSWC PCD), Diving Fleet Systems (S23) branch has an immediate need for rental of a specialized thermal system. The purpose of this system is to cool approximately 4,000 gallons of a ~33% concentration saltwater solution to temperatures below its freezing point, contained within an open-top Conex box. The Contractor will provide a pump that has sufficient GPM capable of cooling 4000 gallons as quickly as possible. NSWC PCD requires specialized subject matter expert guidance and support for the proper setup and connection of the thermal system. The thermal system rental period is estimated to be up to eight (8) weeks.

2.0 APPLICABLE DOCUMENTS

None

3.0 REQUIREMENTS

3.1 Thermal System

The contractor shall provide a high-capacity chiller unit specifically designed or capable of chilling a ~33% concentration saltwater solution to temperatures below its freezing point (i.e., below 0°C / 32°F, accounting for salt depression of freezing point. The system must have a circulation pump suitable for circulating the saltwater solution at the highest feasible Gallons Per Minute (GPM) to facilitate rapid cooling of the 4,000-gallon volume. The contractor must provide all necessary supplies and return piping/hosing of appropriate length and durability for the proposed thermal setup, along with compatible connections/flanges.

3.2 Subject Matter Expertise Support

The contractor shall provide subject matter expertise in chilling specialized diving equipment in a NSWC PCD custom modular 4000-gallon container. The NSWC PCD container is designed to operate diver propulsion / navigation / communication systems in extreme conditions.

3.3 Subject Matter Expertise Training

The contractor shall provide specialized subject matter expert training and guidance on how to properly use the equipment to reach the requested extreme temperatures. The contractor shall provide this training on all specialized equipment and its accessory components such as:

- High-Capacity Chiller Unit with Thermal Control Setpoints and Flow Metering
- Circulation Pump with bypass valves and flow control
- Specialized equipment necessary to reach temperature below freezing point
- Piping/Hosing
- Glycol

3.4 Glycol Drum Purchase

The contractor shall provide the parts identified in the table below to the Naval Surface Warfare Center Panama City Division Special Operations Forces (SOF) Combat Diving (CD) In-Service Engineering Agent (ISEA). Shipping of the below is included in the delivery charge (see CDRL 0005).

Part Number	Description	Qty
N/A	GLYCOL 55 GALLON DRUM	4

3.5 System Set up / Start up

The contractor shall set-up and operationally check the thermal system on site at NSWC PCD. Once the setup is complete the contractor will provide basic operational briefings for NSWC PCD personnel on the safe and effective use of the rented equipment. The contractor shall be subject matter experts on the size of the rental equipment to provide the safe and effective use of it.

3.6 System Cleaning

The contractor shall perform post-rental cleaning, flushing, and decontamination of the chiller unit, and associated hoses due to the use with a concentrated saltwater solution.

3.7 Delivery and Pickup

The contractor shall provide delivery of the chiller unit and all associated equipment to the client's site and subsequent pickup at the conclusion of the rental period.

4.0 GOVERNMENT FURNISHED PROPERTY (GFP)

None

5.0 DATA DELVERABLES

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

6.0 PERIOD OF PERFORMANCE

The period of performance shall be date of award until 90 days after award of purchase order.

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, Defense Federal Acquisition Supplement (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 contract shall 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

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. Refer to DoD 5200.48 for guidance.

7.3 Minimum Requirements for access to CUI

Prior to access, contractor personnel requiring access to Department of the Navy (DON) CUI or "user level access to DON or DoD networks and information systems, system security and network defense systems, or 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" contractors must have clearance eligibility, or submit an Electronic Questionnaire for Investigation Processing (SF 86) to NSWC PCD Security for processing and subsequent adjudication by the DoD Consolidated Adjudications Facility.

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 document designation, not a classification. This designation is used by the 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 Freedom of information Act (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, CUI.

7.5.1 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).

d) 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:

(1) 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).

(2) 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.

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

(4) 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.

(5) 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.

(6) 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.

(7) 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.

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

(9) 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.

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

f) 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.

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

h) 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

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

Technical documentation generated under this Agreement shall carry the following distribution limitation statement. Word processing / electronic files shall have the statements included in the file such that the first page of any resultant hard copy shall display the statements.

DESTRUCTION NOTICE - CLASSIFIED INFORMATION, DESTROY IN ACCORDANCE WITH SECNAVINST 5510.36B, (DON INFORMATION SECURITY PROGRAM) OR DOD 5220.22-M, (NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL). UNCLASSIFIED LIMITED DOCUMENTS, (E.G., FOUO, DISTRIBUTION STATEMENT CONTROL) DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THE DOCUMENT.

DESTRUCTION NOTICE - FOR CLASSIFIED DOCUMENTS, FOLLOW PROCEDURES IN DOD 5220.22-M, NATIONAL INDUSTRIAL SECURITY PROGRAM OPERATING MANUAL, CHAPTER 5, SECTION 7 OR DOD 5200.1-R, INFORMATION SECURITY PROGRAM REGULATION. FOR UNCLASSIFIED, LIMITED DOCUMENTS, DESTROY BY ANY METHOD THAT WILL PREVENT DISCLOSURE OF CONTENTS OR RECONSTRUCTION OF THE DOCUMENT.