STATEMENT OF WORK (SOW)

Confined Space Rescue Training and Certification
for Naval Station Newport Fire Dept.

1.0 Background

Naval Undersea Warfare Center Division Newport (NUWCDIVNPT) requires training for the Naval Station Newport Fire Department (NAVSTA FD) in technical Confined Space (CS) search and rescue. This training is critical to resolve current capabilities gaps, support ongoing operations, and ensure full compliance with OSHA and NFPA safety regulations.

1.1 Places of Performance

Onsite Naval Station Newport, Newport, RI

1.2 Authorized Users

The authorized users for this contract are NUWCDIVNPT, and NAVSTA FD.

1.3 Sponsors

NUWCDIVNPT

.

1.4 Types of Funding

Overhead funds

2.0 Scope

The contractor shall provide the instructors, all training material, and equipment to conduct Confined Space Search and Rescue training and Rope Rescue training that includes both classroom instruction and practical, hands-on exercises. The training program shall cover:

- Hazard recognition and risk assessment
- Atmospheric monitoring and air quality management
- Ventilation techniques
- Lockout/Tag out procedures
- Entry permits and documentation
- Rescue procedures (non-entry and entry rescue)
- Personal protective equipment (PPE) selection and use
- Roles and responsibilities (entrant, attendant, entry supervisor)

3.0 Applicable Documents

The contractor shall perform the tasking required in Section 4.0 in accordance with (IAW) the below Applicable Documents (ADs).

NUMBER	TITLE	REVISION/ DATE	APPLICABLE SOW TASK
3.1	**DoD Issuances**		
3.1.1	DoDI 6055.01 DoD Safety and Occupational Health Program	21 Apr 21	ALL
3.1.2	DoDI 6055.05 Occupational and Environmental Health	31 Aug 18	ALL
3.2	**Navy Issuances**		
3.2.1	OPNAV M-5100.23 Navy Safety and Occupational Health Manual Chp 27	18 Jun 24	ALL
3.3	**Industry Standards**		
3.3.1	OSHA 29 CFR 1910.146 Permit Required Confined Spaces	15 Apr 93	ALL
3.3.2	NFPA 1006 (Technical Rescue Personnel Professional Qualifications)	2021	ALL
3.3.3	NFPA 2500 (Standard for Operations and Training for Technical Search and Rescue Incidents and Life Safety Rope and Equipment for Emergency Services)	2022	ALL

4.0 Technical Requirements

The contractor shall provide the instructors, all digital training material (i.e. thumb-drives with workbooks and supplemental hand-outs), and equipment to train up to sixteen (16) students for the following training. Training dates will be determined by mutual agreement between the contractor and Government prior to training commencement of each training.

Services will be performed onsite at Naval Station Newport for classroom training.

4.1 Rope Rescue - 32 Hours

In accordance with the Applicable Documents in Section 3.0 and using GFI in Section 6.0, the contractor shall provide the classroom training meeting the applicable documentation 3.3.3 standard for Rope Rescue, Chapter 5, in its entirety.

4.1.1 The contractor shall provide two (2) instructors to conduct Rope Rescue training.

4.2 Confined Space Search and Rescue - 48 Hours

In accordance with the Applicable Documents in Section 3.0 and using GFI in Section 6.0, the contractor shall provide classroom training and hands on drills IAW AD 3.2.1 Chapter 27, 3.3.1 and 3.3.3, Chapter 7.

4.3 Certificate of Completion

Upon training completion, the contractor shall:

4.3.1 Provide each successful participant a certificate for each class and documentation verifying training hours and competencies achieved via email, within fourteen (14) calendar days of course completion.

4.3.2 Provide the Government Technical Point of Contact (TPOC), NAVSTANPT Fire Chief and NUWCDIVNPT Confined Space Manager a link to access the completion certificates online.

5.0 Training

Reserved

6.0 Government Furnished Information

RESERVED

7.0 Government Furnished Property

RESERVED

8.0 Security Compliance

8.1 Program Protection

SECURITY: All Contractor personnel shall adhere to the Security provisions of 32 CFR Part 117 – National Industrial Security Program Operating Manual (NISPOM) and the security requirements of the attached DD254. While performing work at a Government Facility, Contractor personnel shall comply with the security regulations of the host facility. Applicable FAR, DFARS, NMCARS clauses, and NAVSEA text shall be adhered to in the performance of this contract. Security incidents shall be promptly reported through the companies Facility Security Officer (FSO), to the Contracting Officer's Representative (COR), Technical Point of Contact (TPOC), and the Cognizant Security Office to NUWCDIVNPT Security.

Controlled Unclassified Information (CUI) including Legacy FOUO and Covered Defense Information (meeting the definition of 48 CFR 252.204–7012(a)) generated and/or provided under this contract shall be marked and safeguarded as specified in DoD Instruction 5200.48, CUI available at:
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/520048p.PDF. Any product containing Covered Defense Information shall be assigned a distribution statement (distribution statements B through F) in accordance with DoDI 5230.24 (Distribution Statements on Technical Documents); and DoDI 5230.24, Enclosure 3 Procedures, available at
https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodi/523024p.pdf

INFORMATION SECURITY: If the work is performed at the Contractor's facility, the Contractor shall implement and maintain security procedures and controls to prevent

unauthorized disclosure of classified information and controlled unclassified information (CUI) and to control distribution of CUI in accordance with National Industrial Security Program Operating Manual (NISPOM) codifying 32 CFR Part 117, NISPOM Rule, and SECNAV M-5510.36B. If the work is performed at the Government's facility, the Contractor shall comply with facility policy.

CUI INCIDENT REPORTING AND RESPONSE: The Contractor shall promptly report any unauthorized, inadvertent, or illegal release or disclosure of CUI to the Contracting Officer's Representative / Technical Point of Contact (TPOC), Procuring Contracting Officer, and the Security Office. Contractor personnel shall coordinate this effort through the relevant industry site FSO.

PUBLIC RELEASE: Any controlled unclassified information pertaining to this contract shall not be released for public dissemination, including posting to any social media sites such as Facebook or Twitter, unless it has been approved for public release by appropriate U.S. Government authority. Proposed public releases shall be submitted for approval prior to release through the appropriate U.S. Government Office.

8.2 Operations Security (OPSEC)

OPSEC is a process that identifies critical information to determine if friendly actions can be observed by adversary intelligence systems, determines if information obtained by adversaries could be interpreted to be useful to them, and then executes selected measures that eliminate or reduce adversary exploitation of friendly critical information.

The Contractor shall develop and implement and update and maintain an OPSEC program to protect controlled unclassified and classified activities, information, equipment, and material used or developed by the Contractor and any subcontractor during performance of the contract. The Contractor shall be responsible for the subcontractor's implementation of the OPSEC requirements. The Contractor developed OPSEC program may include Information Assurance and Communications Security (COMSEC). The OPSEC program shall be in accordance with National Security Presidential Memorandum (NSPM) 28, and at a minimum shall include:

1) Assignment of responsibility for OPSEC direction and implementation.
2) Issuance of procedures and planning guidance for the use of OPSEC techniques to identify vulnerabilities and apply applicable countermeasures.
3) Establishment of OPSEC education and awareness training. To include initial and annual OPSEC training.
4) Provisions for management, annual review, and evaluation of OPSEC programs.
5) Flow down of OPSEC requirements to subcontractors when applicable.

While performing aboard Government sites, the contractor shall: comply with all OPSEC instructions and policies; include OPSEC as part of its ongoing security awareness program and take all required Agency training; Be responsive to the Supporting OPSEC Manager on a non-interference basis; and Protect sensitive unclassified information and activities, which could

compromise classified information or operations, or degrade the planning and execution of operations performed by the Requiring Organization and contractor in support of the mission.

8.3 Electronic Spillage

Electronic Spillage (ES) is defined as a situation where information of higher classification than a system is authorized to process is introduced into that system, intentionally or otherwise. If a Contractor is determined to be responsible for an ES, all direct and indirect costs incurred by the Government for ES remediation will be charged to the Contractor.