

Performance Work Statement (PWS)

Project Title: Cybersecurity for Federal Contracting Professionals

Requiring Activity: NAVSUP FLC San Diego

1.0 Background

Cybersecurity is a critical component of contract planning and administration. Contracting Officers and Contract Specialists at NAVSUP FLC San Diego must be able to navigate complex regulations and identify potential cyber threats throughout the acquisition lifecycle to safeguard government systems and information, with a specific focus on Controlled Unclassified Information (CUI).

2.0 Objective

The objective of this requirement is to provide comprehensive, situational-awareness-level training regarding Cybersecurity for Federal Contracting Professionals. The training will provide a practical understanding of cybersecurity principles, relevant laws and regulations, and considerations for incorporating cybersecurity requirements into solicitations and contracts.

3.0 Scope of Work

The Contractor shall provide all necessary personnel, materials, and services to deliver the "Cybersecurity for Federal Contracting Professionals" course to approximately **forty-five (45) government employees**. The training shall be delivered at a **non-technical/layman's level**, focusing on policy compliance and behavioral changes rather than deep technical configuration.

4.0 Tasks and Requirements

4.1 Course Curriculum

The contractor shall deliver a course that covers the following core topics at a minimum:

- **Overview of Cybersecurity:** Fundamental concepts and terminology, common threats, and the specific role of contracting professionals in cybersecurity management.
- **Cybersecurity Laws and Regulations:** A review of key federal laws and policies applicable to DoN contracts, with emphasis on **DFARS 252.204-7012** and the protection of CUI.
- **Cybersecurity Standards and Frameworks:** An introduction to cybersecurity standards like **NIST SP 800-171** and the **Cybersecurity Maturity Model Certification (CMMC)**, and how they impact acquisitions.
- **Cybersecurity in Acquisition Planning:** Best practices for incorporating cybersecurity requirements into solicitations and evaluating them during contract formation.

4.2 Instructor Qualifications

The contractor shall provide an instructor with demonstrated expertise in **both federal contracting and cybersecurity**. The instructor must have experience teaching adult learners and be able to facilitate discussions and case studies relevant to the Department of the Navy acquisition environment.

4.3 Training Delivery

- **Format:** The course shall be delivered either virtually or in person.
- **Audience:** The training is intended for Government Contract Specialists and Contracting Officers who are not IT professionals.
- **Interactivity:** The course must include interactive elements such as individual or group exercises, facilitated discussions, and case studies.

4.4 Requirements for Successful Completion

Successful completion of the course requires full attendance and active participation in individual and group exercises.

4.5 Student Materials

The contractor shall provide student resource guides, course handouts, and digital or printed reference materials

4.6 Accessibility Requirements

All materials shall be Section 508 of the Rehabilitation Act (29 U.S.C. § 794d) compliant.

5.0 Deliverables

Deliverable	Due Date
Course Presentation/Slides/Student Materials	At least five (5) business days prior to the start of the course.
Roster of attendees who successfully completed the course	Within two (2) business days after course completion.

6.0 Period and Place of Performance

- **Period of Performance (PoP):** The 1-day training shall be scheduled and completed on mutually agreed-upon dates (June or July timeframe).
- **Place of Performance:** The training will be conducted virtually or in person at Naval Station San Diego, CA, as agreed upon.