Advanced Planning Brief to Industry (APBI)

Presented by: Garry Wieneke

CAPT Duncan McKay, USN
Commanding Officer

NAVSEA
WARFARE CENTERS
CRANE

Dr. Angela Lewis, SES
Technical Director

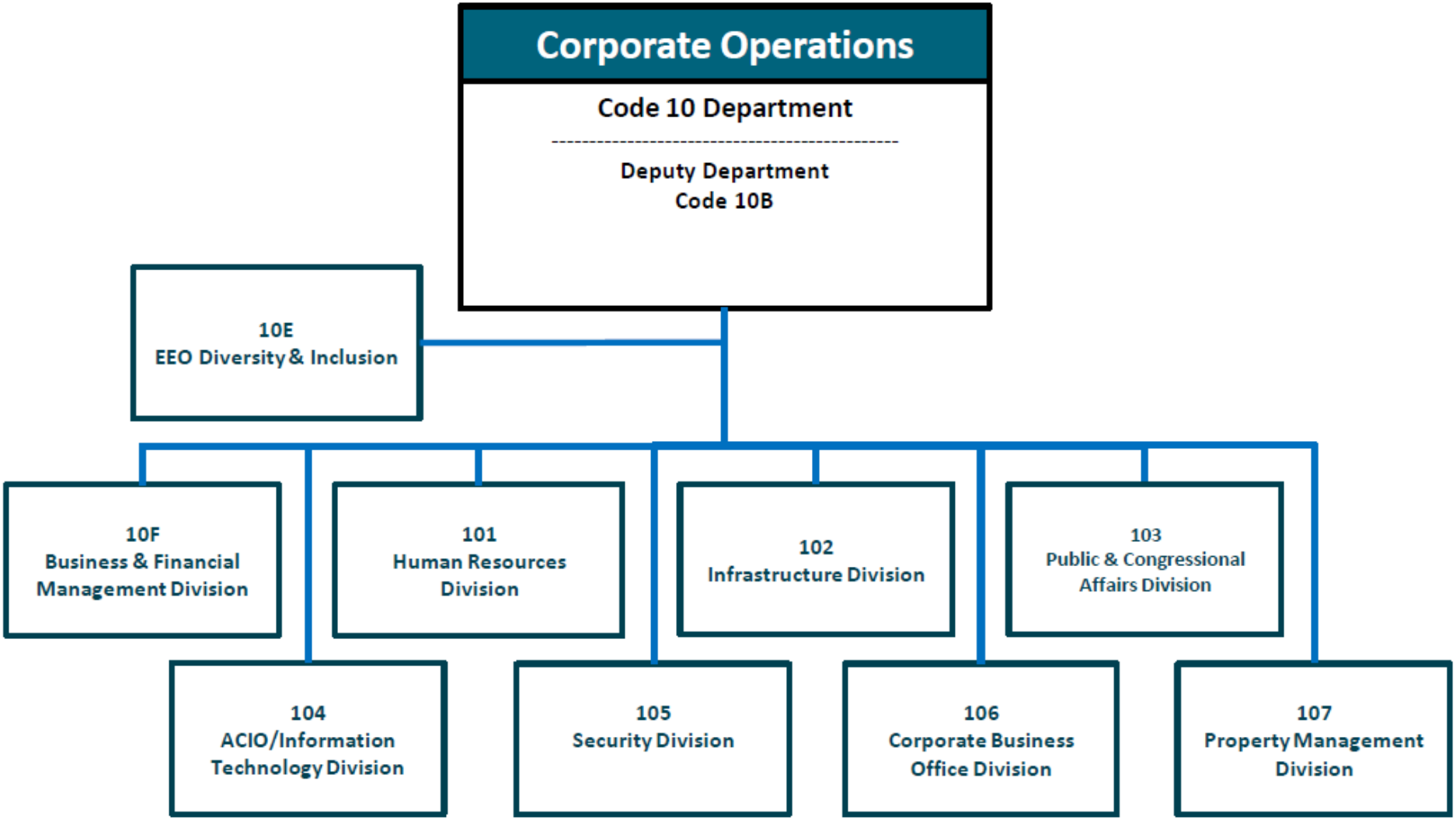
NAVSEA
WARFARE CENTERS
CRANE

Agenda for Corporate Operations

Presenter	Topic
Mr. Garry Wieneke	Corporate Operations Department overview
Mr. Bill Carter	Information Technology Division → Contract Follow-On and other information
Mr. Ryan Johnson	Information Technology Division → Cyber Security Workforce Requirements (CSWF)
Mr. Larry Fink	Cybersecurity → Cybersecurity Maturity Model Certification (CMMC) Requirements
Mr. Terry Reader	Corporate Business Office → Future requirements for analytical methods, data analysis, and predictive modeling
Ms. Barb Strahley	Human Resources Division → Contract Follow-On
Mr. Jesse Beam	Infrastructure Division → Capabilities, Horizontal infrastructure, modular construction, and secure spaces
Ms. Connie Carmichael	Business and Financial Management Division → Contract Follow-On and other information
ALL	Question and answer session

NAVSEA
WARFARE CENTERS
CRANE

Corporate Operations Dept Org Chart



Corporate Operations Dept

NSWC Crane's Corporate Operations Department is a group of talented and trusted professionals who are committed to providing world-class customer service to NSWC Crane's mission areas of Electronic Warfare, Strategic Missions, and Expeditionary Warfare. Everything we do is in pursuit of innovative solutions to meet our mission.

NAVSEA
WARFARE CENTERS
CRANE

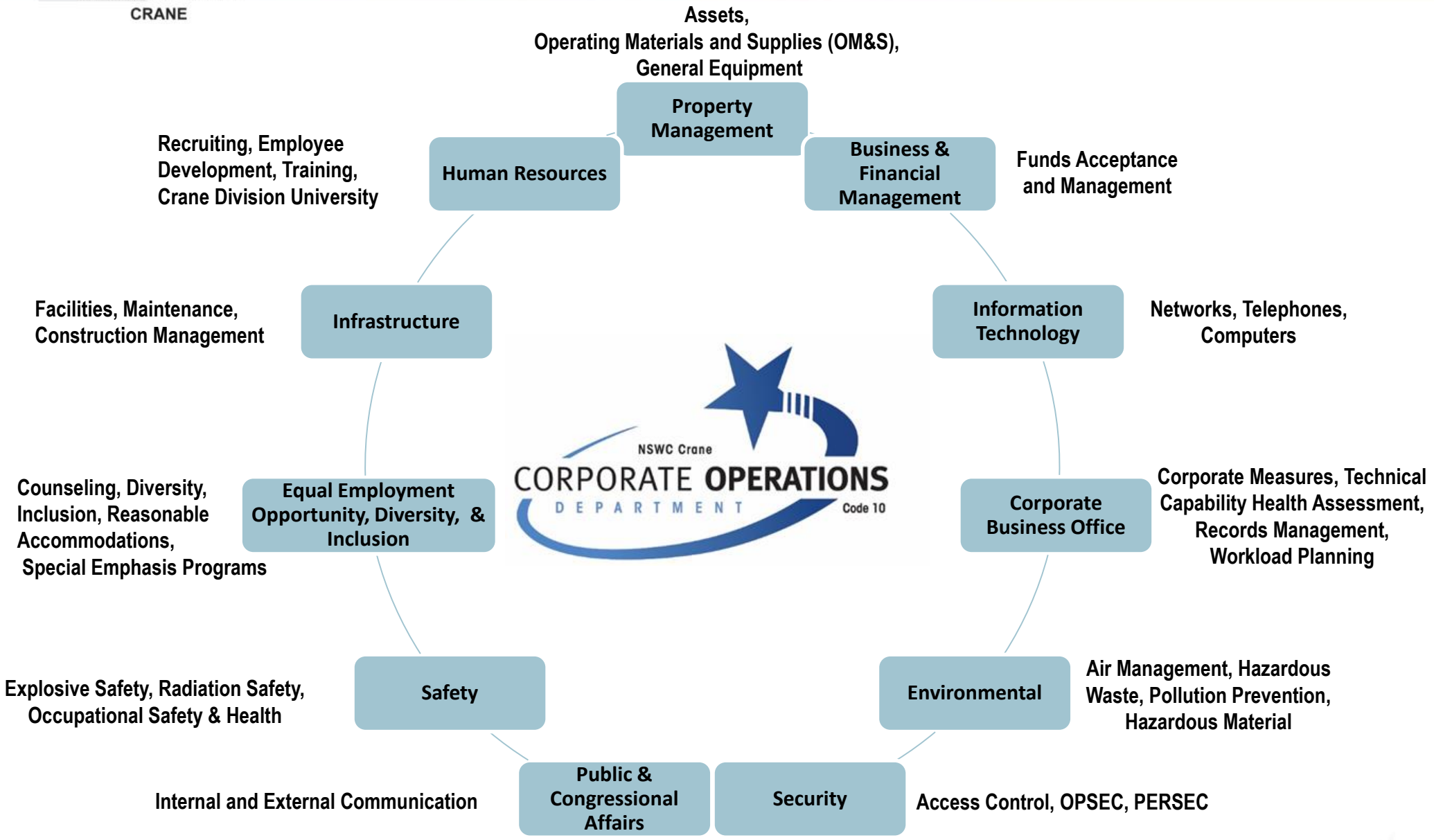
Corporate Operations Dept

- **The Corporate Operations Department is responsible for maintaining a safe, compliant, and mission ready environment.**

- **The Corporate Operations Department Leadership Team works with all levels of management across the Command to provide innovative business solutions focused on meeting the mission.**

NAVSEA
WARFARE CENTERS
CRANE

Business Excellence



NAVSEA
WARFARE CENTERS
CRANE

Crane Division University

CDU
"Achieving Excellence Together Through Education"
CRANE DIVISION UNIVERSITY

GLOBAL DETERRENCE & DEFENSE | SPECIAL WARFARE & EXPEDITIONARY SYSTEMS | SPECTRUM WARFARE SYSTEMS | CORPORATE OPS

CERTIFICATE PROGRAM; ASSOCIATE, BACHELOR, MASTER, DOCTORATE DEGREES

TECHNICAL

PROJECT & PROGRAM MANAGEMENT

LOGISTICS

BUSINESS

MANAGEMENT & SUPERVISION

LEADERSHIP, BASIC KNOWLEDGE, AND CORE VALUES

NAVSEA
WARFARE CENTERS
CRANE

Our Corporate Operations team is committed to Business Excellence through implementation of strategic solutions and integrated planning. We provide business expertise that is integral to NSWC Crane's mission to support our soldiers and sailors.

Advanced Planning Brief to Industry (APBI)

Presented by: Bill Carter

CAPT Duncan McKay, USN
Commanding Officer

NAVSEA
WARFARE CENTERS
CRANE

Dr. Angela Lewis, SES
Technical Director

NAVSEA
WARFARE CENTERS
CRANE

Information Technology Division

- ACIO/Division Management
  - IT Policy & Governance
  - Cybersecurity
  - Program Management
- Deputy Division Management
  - NAVSEA Research Enterprise Network (NREN)
  - IT Asset Management
  - IT Configuration Management
  - IT Quality Management
- IT Operations
  - System, Network, and Database Administrators
  - Desktop Support
  - Data Center Management
  - Webserver & Application Support
  - Cloud Infrastructure
- Information Management
  - Enterprise Software and Application Support (i.e. SharePoint)
  - Software Programmers and Developers (i.e. Power Apps)
  - Service Desk
  - IT Portfolio Management
  - IT Acquisition
- Cybersecurity
  - Computer Network Defense
  - Assessment & Authorization (A&A) Analysis & Validation (RMF Automation)
- Enterprise Services
  - Enterprise & Solution Architects
  - Project Management

IT Support Follow-on Contract

- Length of Contract: Base period of one year with four one-year options.
- Current Task Order: N00178-04-D-4012-N0016417F3003

IT Division Requirements

- Digital Modernization & Transformation
  - Cybersecurity
  - Artificial Intelligence & Machine Learning
  - IT Automation
  - Cloud Migration
  - DevSecOps
  - Data Analytics
- Digital Modernization & Transformation Goals
  - Innovation for a Competitive Advantage
  - Optimization for Efficiencies and Improved Capability
  - Evolving Cybersecurity for an Agile and Resilient Defense posture

IT Support Follow-on Contract

- Special Training/Certificates for Commercial off the Shelf Projects:
  - Ansible Tower
  - F5-BIG IP
  - Cisco
  - Brocade
  - Rubrik
  - Active Directory Federated Services (ADFS)
  - PTC Software Tools (Windchill)
  - CAD tools (Solidworks, Solid Edge, Creo, NX)
  - Model-Based Systems Engineering (MBSE) Tools (Teamwork Cloud, Collaborator, Cameo, Magic Draw, Syndeia, Model Center)
  - Computer Network Defense Tools (SPLUNK, Red Seal, Bluecoat, FirePower, Arista)
  - ServiceNow
  - SharePoint Online
  - Microsoft Power Platform (PowerBI. PowerApps, Power Automate, Power Virtual Agent)

IT Support Follow-on Contract

- Areas of Opportunity
  - IT Automation
  - IT Asset Management
  - DevSecOps
  - Cloud Migration
  - Active Directory Skill Set
  - Software Development Skill Set

IT Support Follow-on Contract

- Cyber Security Workforce Qualifications

  – In accordance with DFARS 252.239-7001, Cybersecurity Contracting Training and Certification herein and SECNAV M-5239.2, Department of the Navy Information Technology and Cybersecurity Workforce Management and Qualification Manual all personnel performing Cyber IT/Cybersecurity functions must be trained and qualified. In addition, personnel shall maintain the appropriate security clearance per SECNAV M-5510.30 to perform the tasks associated with their assigned positions.

  – All positions must meet baseline credentials and maintain appropriate credentials by completing annual continuing education units based on the Cyber IT/CSWF Qualification Matrix (described in SECNAV M-5239.2) associated with the specialty area and proficiency level commensurate with the scope of major assigned duties for the position and tasking being performed.

IT Support Follow-on Contract

- How to help IT become more successful!
  - People
  - Process Improvement
  - Digital Transformation

Advanced Planning Brief to Industry (APBI)

Presented by: Ryan M. Johnson

CAPT Duncan McKay, USN
Commanding Officer

NAVSEA
WARFARE CENTERS
CRANE

Dr. Angela Lewis, SES
Technical Director

CSWF

- Review IT/CSWF membership
- SOW/Contract Verbiage
- CSWF Requirements

NAVSEA
WARFARE CENTERS
CRANE

What is Cyber IT/Cybersecurity?

Per DoD Directive 8140.01, 11 August 2015:

- **Cyberspace Workforce:** Personnel who build, secure, operate, defend, and protect DoD and U.S. cyberspace resources; conduct related intelligence activities; enable future operations; and project power in or through cyberspace. It is comprised of personnel assigned to the areas of cyberspace effects, cybersecurity, cyberspace IT, and portions of Intelligence workforces.
  - **Cyberspace Information Technology (Cyber IT) Workforce –** Personnel who design, build, configure, operate, and maintain information technology, networks, and capabilities. This includes actions to prioritize portfolio investments, architect, engineer, acquire, implement, evaluate, and dispose of information technology and services; as well as information resources management, and the management, storage, transmission, and display of data and information.
  - **Cybersecurity (CS) Workforce –** Personnel who secure, defend, and preserve data, networks, and net-centric capabilities, and other designated systems by ensuring appropriate security controls and measures are in place and taking internal defense actions. This includes access to system controls, monitoring, administration, and integration of cybersecurity into all aspects of engineering and acquisition of cyberspace capabilities.
- Affects ***everyone*** working with Information Technology (IT) or Information Systems (IS); delineates Operations between IT and Cybersecurity.

NAVSEA
WARFARE CENTERS
CRANE

Cyber IT/CSWF Policies/Guidance

- **NIST Special Publication 800-181, National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework, 2017 AUG**
  - Provides a fundamental reference in support of a workforce capable of meeting an organization's cybersecurity needs by using a common, consistent lexicon to describe cybersecurity work by category, specialty area, and work role.
  - "NICE is committed to cultivating an integrated cybersecurity workforce that is globally competitive from hire to retire, prepared to protect our nation from existing and emerging cybersecurity challenges." (NIST SP 800-181, p. 1)

- **DoD Directive 8140.01, Cyberspace Workforce Management, 2015 AUG 11**
  - Reissues and renumbers DoD Directive (DoDD) 8570.01 to update and expand established policies and assigned responsibilities for managing the DoD cyberspace workforce.
  - Unifies the overall cyberspace workforce and establishes specific workforce elements (cyberspace effects, cybersecurity, and cyberspace information technology (IT)) to align, manage and standardize cyberspace work roles, baseline qualifications, and training requirements.

- **SECNAV Instruction 5239.20A, Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification, 2016 FEB 10**
  - Establishes policy and assigns responsibilities for management and qualification of the Department of the Navy (DON) Cyberspace Information Technology and Cybersecurity Workforce (Cyber IT/CSWF) per DoDD 8140.01.

- **SECNAV Manual 5239.2, Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification Manual, 2016 JUN**
  - This manual reissues SECNAVINST 5239.2A to implement policy, update assigned responsibilities, and establish mandatory procedures for uniform identification, management, and qualification of the Department of the Navy (DON) Cyberspace IT and Cybersecurity Workforce (Cyber IT/CSWF).

NAVSEA
WARFARE CENTERS
CRANE

Cyber IT/CSWF Membership

- **Who is part of the Cyber IT/Cybersecurity Workforce?**
  - Contractor personnel performing IT and/or Cybersecurity functions.
  - All personnel with privileged access on any government IT system regardless of connectivity and a signed Privileged Access Agreement (PAA).
  - All other personnel that are performing Cyber IT/Cybersecurity functions (i.e. Software Engineering/Development, System Administration, Cybersecurity, Authorization and Assessment, Test and Evaluation of systems, Systems Engineering/Development, Systems Integration, RMF Package Accreditation, Information Awareness, etc)

NAVSEA
WARFARE CENTERS
CRANE

SOW Verbiage for Contracts

3.X.X Cyber Security Workforce (CSWF) Qualifications and Reporting

Each Technical Instruction (TI) will be reviewed by the Naval Surface Warfare Center Crane Division CSWF Program Manager and a determination made regarding applicability of CSWF requirements to the tasking identified. If it is determined the tasking identified in the TI requires personnel to Cyber IT/Cybersecurity functions the requirements of DFARS 252.239-7001, Information Assurance Contracting Training and Certification shall apply.

3.X.X.X Cyber Security Workforce Qualifications

In accordance with DFARS 252.239-7001, Information Assurance Contracting Training and Certification herein and SECNAV M-5239.2* dated June 2016, all personnel performing Cyber IT/Cybersecurity functions must be trained and qualified. In addition, personnel shall maintain the appropriate security clearance per SECNAV M-5510.30 to perform the tasks associated with their assigned positions.

All positions with Cyber IT/Cybersecurity functions whether primary or additional/embedded duties have a Specialty Area and Proficiency Level identified within the Special Skills section of each TI.

The contractor is required to:

1. Earn and maintain appropriate credentials from the Cyber IT/CSWF Qualification Matrix (described in SECNAV M-5239.2*) associated with the specialty area and proficiency level commensurate with the scope of major assigned duties for the position and tasking being performed.

2. Participate in continuous learning program as described in SECNAV M-5239.2. All contractor support personnel supporting CSWF tasking shall at a minimum complete 20 hours of Cyber IT/CSWF related continuous learning (CL) annually.

The baseline qualifications for each specialty area/proficiency level are identified in Appendix 4 of SECNAV M-5239.2*. If privileged access to Operating Systems is required, the contractor shall complete a privileged access agreement, SECNAV 5239/1, and submit it to the COR (Attachment X). Contractor personnel shall obtain the appropriate DON approved baseline job qualification standard prior to being engaged. Contractors have up to 6 months to obtain any additional qualifications required for their position to include but not be limited to applicable operating system/computing environment training if required. A copy of the certificate of completion shall be provided to the COR.

Per SECNAV M-5239.2, unless expressly provided for in the Task Order, all responsibility for training that is required for the contractor to maintain a specific expertise, commercial certification, or continuous learning is the sole responsibility of the contractor employee and or the contractor's employer. Only Government specific CSWF training may be directly charged to the Task Order and only if authorized by the TI.

* Contractor shall use SECNAV M-5239.2 until DFARS Clause- 252.239-7001 is updated, specifically with regards to vendor certifications. At that time education and military training may be used in regards to contractor qualifications.

3.0.X.X Cyber Security Workforce Reporting

The contractor shall provide a list of all personnel assigned to TI's with personnel performing Cyber IT/Cybersecurity functions as a part of the monthly Contractor's Progress, Status, and Management Report (A00X). The report shall include employee name, TI#, list of applicable Cyber IT/Cybersecurity function category/level (see TI), required certifications and fulfillment status and CL status (See sample format, Attachment Y).

New hire information for tasking requiring Cyber IT/Cybersecurity functions shall be submitted to the COR at least 7 days prior to employee beginning performance of any Cyber IT/Cybersecurity functions. New hire information shall include name, TI#, list of applicable Cyber IT/Cybersecurity functions category/level, required certifications and fulfillment status to include a copy of the certification documentation. Contractors are encouraged to provide new hire information to ensure Government concurrence with qualification to perform Cyber IT/Cybersecurity functions. Per DFARS 252.239-7001(c), "Contractor personnel who do not have proper and current certifications shall be denied access to DoD information systems for the purpose of performing information assurance functions." and therefore may not be allowed to charge to the Task Order.

A00X	Cyber Security Workforce (CSWF) Report	DI-MGMT-82160

3.X.X.X Contractor Information Assurance (IA) Training and Certification

The Contractor shall ensure that personnel who are categorized as working within the DoD IA workforce meet the appropriate requirements of SECNAV M-5239.2. Cyber Security Workforce requirements IAW DFARS 252.239-7001 are applicable to this tasking. See SOW 3.0.2 for CSWF qualification and reporting requirements.

Policies and Guidance in Contracts

- **DFARS Clause- 252.239-7001 Information Assurance Contractor Training and Certification**
- **DoD Manual 8570.01-M**
  - Contracts performing cyber tasking with the 8570.01 guidance referenced must have CSWF verbiage in Special Skilled required section of each cyber TI
  - Will be a set list of vendor certification that satisfy the baseline requirement
- **SECNAV M-5239.2**
  - Contracts performing cyber tasking with the 5239 guidance referenced must have CSWF verbiage calling out specialty area and proficiency level in special skills required section of each cyber TI
  - Each specialty area has a defined set of certification that may satisfy the baseline requirement
  - CSWF team worked with contracting to create a hybrid clause for contracts that allows contracts to be compliant with both 8570 and 5239 due to DOD not yet updating DFARS clause. This clause language is found in the SOW

Cyber IT/CSWF Qualification/Training Requirements

- ***All Contractor*** workforce members must satisfy the baseline requirement prior to performing cyber tasking on a contract.
- ***All*** workforce members are required to complete 20 hours of Navy approved Continuous Learning(CL)/Continuous Education Unit (CEU) activities per calendar year. If not completed, member will no longer be permitted to perform cyber tasking.
- Workforce members with privileged access on any government IT systems are required to obtain approved training on **ALL** Operating System(OS) /Computer Environment (CE) technologies which are identified on their signed Privileged Access Agreement (PAA).

  – Note: Unless specifically in the contract, all commercially available training costs are the responsibility of the contractor and shall not be charged to the government

Questions?

NSWC Crane POC:

Tyler Brough

Cyber IT/Cybersecurity Workforce Program Manager

CRAN_CSWFManagement_Team@navy.mil

tyler.j.brough1@navy.mil