THE SECRETARY OF THE NAVY

SECNAV M-5239.2
JUNE 2016

DEPARTMENT OF THE NAVY

CYBERSPACE INFORMATION TECHNOLOGY AND CYBERSECURITY WORKFORCE MANAGEMENT AND QUALIFICATION MANUAL

PUBLISHED BY

DEPARTMENT OF THE NAVY CHIEF INFORMATION OFFICER

Table of Issuance and Revisions/Changes

SECNAV Manual	**Basic Issuance Date**
5239.2	May 2009
	June 2016

FOREWORD

This manual implements the policy established in Secretary of the Navy Instruction (SECNAVINST) 5239.20A, Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification.

This manual revises and reissues SECNAV Manual 5239.2, DON Information Assurance (IA) Workforce Management; it is effective immediately and should be read in its entirety. This revision identifies major changes to the DON Cyberspace IT/Cybersecurity Workforce (Cyber IT/CSWF) Management and Qualification Program. It updates and clarifies the position and personnel coding process, sets qualifications criteria, and establishes program management procedures. Appendix 4, Cyber IT/Cybersecurity Workforce Qualification Matrix, was added to this manual to clarify qualification requirements and options.

This manual details the general cybersecurity training required by all Department of the Navy (DON) authorized users and the specific qualifications required by personnel identified as "Core" Cyber IT/CSWF.

This manual may be accessed through the DON Issuances Web site: http://doni.documentservices.dla.mil/. Points of contact are provided below for those seeking additional information.

DON Chief Information Office
1000 Navy Pentagon
Washington, DC 20350
www.doncio.navy.mil

DON/Assistant for Administration Directives and Records Management Division
1000 Navy Pentagon
Washington, DC 20350
Commercial: (703) 601-1018

RAY MABUS

Table of Contents

INTRODUCTION

1. PURPOSE. This manual reissues reference (a) in accordance with the authority conferred by references (b), (c), and (d) 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). References (a) through (t) pertain to Cyber IT/CSWF and are contained in Chapter 1.

2. APPLICABILITY. This manual applies to the Office of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), all U.S. Navy (USN) and U.S. Marine Corps (USMC) installations, commands, activities, and field offices, and all other organizational entities within the DON.

3. POLICY. It is DON policy, in accordance with reference (c), that:

a. Commanders, Commanding Officers (COs), Officers in Charge (OIC), and Directors, hereinafter referred to as “Commanders of DON organizations,” shall identify all positions requiring performance of Cyber IT/CS functions.

b. Cyber IT/CSWF functions must be identified and managed, and personnel performing cybersecurity functions will be appropriately screened, in accordance with this manual and reference (e). They will be trained and qualified in accordance with reference (f) and supporting issuances. Qualified Cyber IT/CSWF personnel must be identified and integrated into all phases of the system development life cycle. The guidance and standards detailed in the qualification requirements and Cyber IT/CSWF matrices apply to positions and personnel designated as Cyber IT/CSWF.

c. The DON workforce requires differing levels of cyber knowledge, skills, and abilities (KSAs). For the purpose of this manual these levels are:

(1) Authorized User: Requires general computer skills and baseline understanding of cybersecurity to conduct work that is not IT or cybersecurity focused. The general DON workforce - military, civilian, and contractor – are Authorized Users.

(2) Enhanced User: An Authorized User (military, civilian or contractor) who requires detailed knowledge of Cyber IT and/or cybersecurity to support work in the development, maintenance, or operation of DON systems, including weapons, tactical, electronic and electrical services, navigation, and engineering. Enhanced Users possess advanced Cyber IT/CS knowledge and abilities centered on particular professional areas.

(3) Core Cyber IT/CS User: An Authorized User (military, civilian, or contractor) who requires KSAs in both technical and managerial aspects of Cyber IT/CS. The Core User group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing

capabilities, and communications. It also includes personnel who manage risk and protect DON networks and information systems (IS).

d. Each Authorized, Enhanced, and Core User of DON IS must maintain the appropriate security clearance; have a current user access agreement (e.g., System Authorization Access Request (SAAR)) and, if applicable, a Privileged Access Agreement (PAA); and complete approved cybersecurity awareness training prior to accessing DON networks. Commanders of DON organizations may add specific Service and local cybersecurity policies and procedures to the standardized baseline training. Cybersecurity awareness training includes initial awareness orientation and annual refresher training.

e. In addition to the requirements for Authorized Users, each Enhanced User of DON systems must meet the standards established in workforce qualification and training requirements for specific billet or position types (e.g., acquisition, intelligence, or communication). Enhanced Users should also receive additional Cyber IT/CS training related to their specific tasks. Additional Cyber IT/CS training should be included in Enhanced Users' overall qualification programs and detailed in Navy and Marine Corps guidance. Commands should provide Cyber IT/CS training for their Enhanced User personnel that addresses command missions and needs.

f. All Cyber IT/CSWF personnel must be trained and qualified and must maintain the appropriate security clearance per reference (e) to perform the tasks associated with their assigned positions. This includes demonstration of foundational knowledge attained through completion of training, education, or certification programs and final qualification through a demonstration of ability to perform cybersecurity job tasks (e.g., Job Qualification Requirement (JQR)).

g. Cyber IT/CSWF qualification requirements will be documented in a qualification matrix, based upon a DON Cyber IT/CS framework, and structured by Cyber IT/CSWF Category and Specialty Area (SA).

h. Foundational Cyber IT/CS knowledge will address risk management, cybersecurity concepts, operating system/computing environment (OS/CE) concepts, and technical information.

i. Foundational Enhanced User and Core Cyber IT/CS knowledge attainment may be acquired through completion of approved military training, academic degrees, or commercial cybersecurity certifications.

j. Cyber IT/CSWF qualifications will be aligned to required proficiency levels.

k. All Cyber IT/CSWF personnel will be required to maintain qualification currency through participation in an annual continuous learning (CL) program in accordance with reference (o).

l. A Cyber IT/CSWF Program Manager (Cyber IT/CSWF-PM) role will be established. Only a military member or government civilian may serve as a Cyber IT/CSWF-PM. Only U.S.

citizens may serve as Cyber IT/CSWF-PMs. This role will be responsible for the administration of an organization's Cyber IT/CSWF Program. Whenever possible, the Cyber IT/CSWF-PM role shall be a primary duty. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization, or by the Command Information Systems Security Manager (ISSM).

m. The tracking of Cyber IT/CSWF positions and workforce personnel qualification status (including CL) will be captured in the DON Cyber IT/CSWF enterprise tracking tool (Total Workforce Management Services (TWMS)). The DON/Navy/Marine Corps authoritative personnel and readiness databases will be the sources for Workforce qualification status readiness reporting. Commanders of DON organizations will be accountable for accurately maintaining their Cyber IT/CSWF status within DON/Navy/Marine Corps authoritative personnel and readiness databases.

n. Cyber IT/CSWF personnel training and qualification compliance shall be monitored by the Cyber IT/CSWF-PM. A Cyber IT/CSWF member who fails to maintain necessary qualifications shall be removed from cybersecurity positions and may only return with the consent of the organization's Commander and a waiver approved by the appropriate DON Deputy Chief Information Officer (CIO). In addition to removal from cybersecurity positions, failure to maintain required qualifications will result in counseling and proper documentation by the Cyber IT/CSWF-PM and chain of command. Personnel failing to maintain qualifications create a weakened security posture and will negatively affect an organization's Cybersecurity Inspection (CSI) ratings.

o. All personnel with "privileged access" will be required to acknowledge their responsibilities with DON approved SAAR indicating Privileged Access and PAA (see Appendices 1 and 2). Personnel with the Privileged Access block checked on their SAAR will be designated as Privileged Users and members of the Cyber IT/CSWF. The positions to which they are assigned must be designated as Cyber IT/CSWF positions. These agreements must be reviewed, updated, and signed annually and must identify the specific system, network, or application to which an individual has privileged access. A signed copy of the agreement shall be maintained by the network administrator as part of the official network records. Personnel no longer requiring privileged access shall have their records modified to reflect a change in the access granted. The DON Cyber IT/CSWF enterprise tracking tool (TWMS) will be appropriately updated when a member no longer requires privileged access or is removed from the Cyber IT/CSWF.

p. A privileged user may be a member of either the Cyber IT or CSWF category. Designation is based upon the tasks and authorities assigned to the position a person holds.

q. Navy and Marine Corps Reserve Commands/units will:

(1) Identify all Cyber IT/CS Reserve Force personnel.

(2) Electronically track all Reserve Force Cyber IT/CS billets and personnel.

(3) Ensure all Cyber IT/CS Reserve personnel maintain appropriate security clearance, receive the designated CS training, and hold necessary certifications.

(4) Implement Cyber IT/CSWF Management Programs.

(5) Develop procedures for immediate notification and recall of assigned Cyber IT/CS personnel.

(6) Ensure all Reserve Force Personnel take the initial Department of Defense (DoD) CS Awareness course and annual refresher.

r. Manager's Internal Control Program (MICP). Per reference (g), it is DON policy that each Major Assessable Unit (MAU) and/or command establish a MICP to evaluate and report on the effectiveness of Internal Controls (ICs) throughout their organizations, and make corrections when necessary. MAUs and/or commands shall include Cyber IT/CSWF Management and Qualifications when performing IC and risk assessments.

4. RESPONSIBILITIES. See Chapter 2.

5. PROCEDURES. Chapter 3 provides the standards and procedures required to identify, document, and track cybersecurity positions and the qualifications of personnel assigned to them as well as for cybersecurity contracted services support.

6. RECORDS MANAGEMENT. Records created as a result of this manual, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.

7. INFORMATION COLLECTION REQUIREMENTS. Reporting of Cybersecurity position information and workforce personnel training and qualification status (to include CL status) will be accomplished utilizing a DON CSWF enterprise tracking tool (TWMS). The DON/Navy/Marine Corps personnel and readiness authoritative databases will be the source for Workforce qualification status readiness reporting.

8. REPORTS. The reporting requirements contained in Chapter 2, paragraphs 16a and 16b are exempt from reports control per SECNAV M-5214.1 of December 2005, Part IV paragraph 7c.

9. FORMS. SECNAV 5239/1 (03-2016), Information System (IS) Privileged Access Agreement (PAA) and Acknowledgment of Responsibilities is available electronically from Naval Forms Online at: https://navalforms.documentservices.dla.mil/web/public/home

10. RELEASABILITY. **Cleared for public release**. This SECNAV M-5239.2 is available on the Internet from the DON Issuances website at https://doni.documentservices.dla.mil/.

11. EFFECTIVE DATE. This manual is effective 27 June 2016.

CHAPTER 1

REFERENCES

a) SECNAVINST 5239.20A, Department of the Navy Cyberspace Information Technology and Cybersecurity Workforce Management and Qualification, 10 February 2016
b) 44 U.S.C. Chapter 35, Subchapter II and III (also known as the "Revised Federal Information Security Modernization Act (FISMA) of 2014")
c) SECNAVINST 5239.3C, Department of the Navy Cybersecurity Policy, 2 May 2016
d) SECNAVINST 3052.2, Cyberspace Policy and Administration within the Department of the Navy, 6 March 2009
e) SECNAV M-5510.30, Department of the Navy Personnel Security Program, 30 June 2006
f) DoD Directive 8140.01 , Cyberspace Workforce Management, 11 August 2015
g) SECNAVINST 5200.35F, Department of the Navy Managers' Internal Control Program, 21 July 2014
h) DoD Instruction 8500.01, Cybersecurity, 14 March 2014
i) DoD Acquisition Regulations System (DFARS) 48 CFR Parts 239 and 252 RIN 0750-AF52, Supplement; Information Assurance Contractor Training and Certification (DFARS Case 2006-D023), 22 January 2007
j) DoD Instruction 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 2014
k) Cybersecurity Data Element Standard in the OPM "Guide to Data Standards", 9 July 2013
l) DoD Directive 5205.02E, DoD Operations Security (OPSEC) Program, 20 June 2012
m) DoD Instruction 1100.22, Policy and Procedures for Determining Workforce Mix, 12 April 2010
n) DoD Manual 5200.01 Volume 3, Enclosure (5), DoD Information Security Program: Protection of Classified Information, 24 February 2012
o) SECNAVINST 1543.2, Cyberspace/Information Technology Workforce Continuous Learning, 30 November 2012
p) DoD 5500.7-R, Joint Ethics Regulation (JER), 30 August 1993 (as amended)
q) DoD Instruction 1400.25, Volume 410 DoD Civilian Personnel Management System, 25 September 2013
r) DoD Instruction 8320.03, Unique Identification (UID) Standards for Supporting Department of Defense Net-Centric Operations, 4 November 2015
s) National Security Presidential Directive (NSPD)–54/Homeland Security Presidential Directive (HSPD)-23, Cybersecurity Policy, 8 January 2008
t) CNSSI No. 4009, IA Glossary, 26 April 2010

List of Cybersecurity-related laws, regulations, and DoD policies:
http://iase.disa.mil/index2.html

DON Issuances:
https://doni.documentservices.dla.mil

CHAPTER 2

RESPONSIBILITIES

1. DON CHIEF INFORMATION OFFICER (DON CIO).

The DON CIO shall:

a. Carry out the Cyber IT/CSWF management responsibilities assigned by references (a) and (b) to the head of each Federal Agency and those outlined in references (c) and (d). Accordingly, the DON CIO shall ensure DON compliance with the Cyber IT/CSWF requirements of references (f) and (h) and related Cyber IT/CSWF policies, procedures, standards, and guidelines.

b. Set DON standards and develop Cyber IT/CSWF policies, CSWF identification, education, training, certification and qualification per references (i) and (j). This includes oversight of the DON Cyber IT/Cybersecurity Workforce Qualification Program (Cyber IT/CSWFQP) and the DON Cybersecurity Awareness Program.

c. Set DON standards and policy for CS user awareness training.

d. Serve as the DON Cyber IT/CSWF management and qualification office of primary responsibility (OPR).

e. Establish criteria and processes for selecting training, education, and certification programs.

f. Collaborate with DON stakeholders to establish metrics to monitor and validate compliance with this directive as an element of mission readiness.

g. Chair the Cyber IT/CSWF Management, Oversight, and Compliance Council (Cyber IT/CSWF MOCC).

2. DON DEPUTY CIO (DDCIO) (NAVY) AND DDCIO (MARINE CORPS).

The DDCIO (Navy) and DDCIO (Marine Corps) shall:

a. Co-Chair and support the Cyber IT/CSWF MOCC.

b. Develop and implement Cyber IT/CSWF management and qualification programs, guidance, and procedures within their respective Services.

c. Provide support to the DON Cyber IT/CSWF Leader, DON CIO. Collaborate with the personnel and training command OPRs in the development of Service unique military and civilian training and career management. Additionally, ensure the core Cyber IT/CSWF training, qualification, education, and management requirements are met and consistent with DON direction as follows:

(1) Develop a strategy for Cyber IT/CSWF workforce development to include recruitment, retention, and development of Cyber IT/CSWF personnel throughout their careers.

(2) Provide for and electronically track initial Cybersecurity orientation and annual awareness training of all authorized users.

(3) Identify total force structure/positions performing Cyber IT/CS functions by category and SA per reference (f).

(4) Electronically track Cyber IT/CSWF personnel who perform Cyber IT/CS functions to ensure that Cyber IT/CS positions are staffed with trained and qualified personnel.

(5) Identify Cyber IT/CS functions that may be performed by contractors, and provide contract language requirements to be included in their statement of work (SOW) and/or contract, and ensure that all DON contracts, requiring performance of cybersecurity functions, include the requirement to report contractor personnel's cybersecurity qualification status per reference (k).

(6) Ensure personnel obtain the appropriate background investigation and security clearance per reference (e) prior to granting unsupervised privileged access or management responsibilities to any DON system. Contractors must also meet the security eligibility requirements.

(7) Collect metrics and submit reports to the DON CIO to support planning and analysis of the Cyber IT/CSWF and annual Federal Information Security Management Act (FISMA) reporting.

(8) Provide oversight and coordination for necessary resourcing and implementation of Cyber IT/CSWF management plans and processes.

(9) Identify all personnel using the Office of Personnel Management (OPM) Cybersecurity Data Element and DoD Inherently Governmental/Commercial Activity Codes in Authoritative Data Sources (ADS) to include the applicable Non-Appropriated Fund (NAF) manpower system per reference (k).

(10) Coordinate to ensure appropriate Cybersecurity content is included in officer accession programs; Flag, Commander/Commanding/Executive Officer (CO/XO), and Warrant Officer training; and professional military education. The training will be developed to provide leadership understanding of the critical importance of cybersecurity to the successful execution of the operational mission.

(11) Coordinate the implementation of the DON Cyber IT/CSWF Program within their respective service.

3. DON SENIOR INFORMATION SECURITY OFFICER (SISO).

The DON SISO (formerly Senior Information Assurance Officer (SIAO)) shall:

a. Implement and enforce the Risk Management Framework within the DON component Cybersecurity Program.

b. Establish and oversee a team of cybersecurity professionals qualified in accordance with reference (h), responsible for conducting security assessments. DON SISOs may task, organize, staff, and centralize or direct assessment activities to representatives as appropriate. Regardless of the adopted model, the SISO is responsible for assessing quality, capacity, visibility, and effectiveness.

4. DON CYBER IT/CS WORKFORCE OFFICES OF PRIMARY RESPONSIBILITY (OPR).

The DON Cyber IT/CSWF OPRs shall:

a. Coordinate the implementation and sustainment requirements of this manual to include supporting tools and resources (e.g., conferences, website, database integration, workforce identification).

b. Coordinate with DON CIO and DON military personnel and training system program management regarding development of proper Cyber IT/CSWF management processes and systems as well as funding to support Cyber IT/CSWF management ADS and tools. The DON OPRs will also coordinate directly with the Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN (M&RA)) and DON Manpower Functional Area Manager to determine requirements for, and the development of, the workforce interim DON Cyber IT/CSWF enterprise tracking tool (TWMS) for Cyber IT/CSWF management and reporting.

c. Ensure that Cyber IT/CSWF positions are captured in Total Force Manpower Management System (TFMMS) for the Navy positions and Total Force Structure Management System (TFSMS) for the Marine Corps positions.

d. Ensure Cyber IT/CSWF manpower and personnel information including personnel qualification status (to include CL status) is captured in the DON Cyber IT/CSWF enterprise tracking tool (TWMS).

5. DON CYBER IT/CS WORKFORCE OFFICES OF PRIMARY RESPONSIBILITY (OPR) Cyber IT/CSWF PROGRAM MANAGER (Cyber IT/CSWF-PM).

The DON OPR Cyber IT/CSWF-PM shall:

a. Coordinate the identification, tracking, and qualifications of Cyber IT/CSWF personnel within their service. This includes oversight, management, and the identification of education, training, certification, and qualification of Cyber IT/CSWF individuals.

b. Coordinate with intelligence, logistics, aviation, submarine, surface, and other communities regarding development of proper Cyber IT/CSWF management processes and systems to include funding to support these workforce qualifications. The Service OPRs will also coordinate directly with the service manpower and personnel organizations to advise on proposed manpower and personnel changes. The OPR Cyber IT/CSWF-PM will coordinate with service manpower and personnel organizations to ensure that the required processes and data needed for Cyber IT/CSWF management are included in service personnel and training tools. If the ADS do not fully support Cyber IT/CSWF management needs, determine which additional tools are necessary to support workforce management.

c. Coordinate with Navy Echelon II (Ech II) and Marine Corps Major Subordinate Commands (MSC) to define Cyber IT/CSWF position responsibilities and requirements.

6. DON AUTHORIZING OFFICIALS (AO).

The DON AO (formerly known as Principal Accrediting Authority) shall:

a. Be trained, qualified, and appointed in writing for each DoD IS, DoD partnered system, and Platform IT (PIT) system operating within or on behalf of the DON and ensure that the systems are authorized in accordance with reference (j). Relevant PIT expertise must be a factor in the selection and appointment of AOs responsible for authorizing PIT systems.

7. ECHELON II/MAJOR SUBORDINATE COMMAND INFORMATION OFFICER (Ech II/MSC COMMAND IO).

The Echelon II/MSC Command IO shall:

a. Be a key position for supporting Cyber IT and Cybersecurity efforts and effective implementation of associated plans. They serve as the principal advisor to the Commander for the alignment of business processes through implementation of enterprise architecture, IT planning procedures, and the protection of mission critical and mission essential systems through strengthened cybersecurity management and technical controls.

b. Establish and maintain a reporting relationship with ISSM for all networks, systems, applications, and databases under their control.

c. Establish and maintain a reporting relationship with Cyber IT/CSWF-PM for all subordinate unit CSWF personnel assigned to ensure core workforce training, certification, education, and management requirements are identified and tracked in accordance with DON direction.

d. Provide the information required to develop and submit Cyber IT and Cybersecurity training, education, and qualification budget requirements.

e. Be a U.S. citizen. Non U.S. citizens and contractors may not serve as Command IO.

8. ECHELON II/MAJOR SUBORDINATE COMMAND CYBER IT/CS WORKFORCE PROGRAM MANAGER (Cyber IT/CSWF-PM).

The Cyber IT/CSWF-PM shall:

a. Be responsible for the Cyber IT/CSWF Program within their respective domain and serve as the central Cyber IT/CSWF-PM for organizational Cyber IT/CSWF-PMs under their purview.

b. Be accountable for the effectiveness of the Cyber IT/CSWF Management and Qualification Program.

c. Be a U.S. citizen. Non U.S. citizens and contractors may not serve as Cyber IT/CSWF-PM.

9. ECHELON II/MAJOR SUBORDINATE COMMAND INFORMATION SYSTEMS SECURITY MANAGER (ISSM).

The ISSM (formerly known as IA Manager (IAM)) shall:

a. Be responsible (with the review and approval of the responsible CIO) for ensuring that all cybersecurity components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

b. Be trained, qualified, and appointed in writing for DON IS and PIT systems operating within or on behalf of the DON and ensure that the systems are authorized in accordance with reference (j).

c. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.

d. Serve in this ISSM position as his/her primary duty at the organization (not an embedded or collateral duty).

e. Be a U.S. citizen. Non U.S. citizens and contractors may not serve as ISSM.

f. Be appropriately cleared to DON guidance.

g. Serve as the organizational Cyber IT/CSWF-PM, if appropriate (not mandatory).

10. ECHELON II/MAJOR SUBORDINATE COMMAND INFORMATION SYSTEM SECURITY OFFICER (ISSO).

ISSOs (formerly known as IA Officers (IAO)), shall:

a. Assist the ISSMs in meeting their duties and responsibilities.

b. Coordinate with the Command Security Manager to ensure that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS and PIT systems under their purview before being granted access to those systems.

c. Fulfill both the ISSM and the ISSO roles when circumstances warrant.

d. Be a U.S. citizen. Non U.S. citizens and contractors may not serve as ISSO.

11. <u>COMMANDERS, COMMANDING OFFICERS, AND OFFICERS IN CHARGE</u>.

Commanders, COs, and OIC shall:

a. Be responsible for Cyber IT and Cybersecurity training and qualification compliance.

b. Ensure the command has a Cyber IT/CSWFQP that ensures training managers work with the Cyber IT/CSWF-PM to meet shared Cyber IT/CSWF tracking, training, qualification, and reporting responsibilities.

c. Ensure Cyber IT/CSWF Individual Development Plans (IDPs) are created that detail specific cybersecurity training and qualifications required for compliancy. See Appendix 6.

d. Review the cyber IT and cybersecurity structure of the command and identify appropriate staffing requirements.

e. Designate a Cyber IT/CSWF-PM. The Cyber IT/CSWF-PM will be responsible for the administration of organization's Cyber IT/CSWF Program. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization or the Command ISSM.

f. Ensure Cyber IT/CSWF-PMs are assigned as a primary duty (not collateral duty).

g. Promote the professional development and qualification of employees who carry out cyber IT and cybersecurity responsibilities.

h. Stabilize workforce rotation in the workplace so trained cyber IT and cybersecurity personnel are assigned to cyber IT and cybersecurity jobs commensurate with their qualifications.

i. Ensure all IS users (including contractors) are appropriately trained in accordance with references (a), (c), and (j) to fulfill their cybersecurity responsibilities before allowing them system or network access.

j. Ensure cyber IT and cybersecurity contractor personnel have the appropriate appointment letter, cybersecurity qualification, and background investigation. Contracting Officer's

Technical Representative must ensure the command contracting officer is aware of contractor personnel not meeting appointment, qualification, or investigation requirements. Command contracting officer will ensure current and future contract SOW or Performance Work Statement (PWS) have sufficient language that requires contractor personnel to meet appointment, qualification, and investigation requirements.

k. Inform the OPR Cyber IT/CSWF-PM of personnel who are not in compliance and their status.

l. Develop a local Cyber IT/CSWFQP implementation plan.

m. Ensure the local Cyber IT/CSWF is identified and documented in approved databases.

n. Ensure the local Cyber IT/CSWF members are trained and properly qualified.

o. Authorize the Command IO to oversee the Cyber IT/CSWFQP.

p. Empower the Command Cyber IT/CSWF-PM to ensure compliance.

q. Assign personnel and training responsibilities to local human resources, administrative, and training officers to carry out Cyber IT/CSWF management.

r. In the event a Cyber IT/CSWF member fails to achieve qualification compliance, notify the Cyber IT/CSWF member of his/her status and any required remediation. The command shall put the member in a waiver status (not to exceed 6 months); pending review of competencies and potential movement to a non-Cyber IT/CSWF position. If a non-Cyber IT/CSWF position is not available, the employee will be subject to other action, up to and including removal.

12. COMMAND CYBER IT/CYBERSECURITY WORKFORCE PROGRAM MANAGER (Cyber IT/CSWF-PM).

The Command Cyber IT/CSWF-PM shall:

a. Be responsible for the administration of organization's Cyber IT/CSWF Program. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization or by the Command ISSM.

b. The Cyber IT/CSWF-PM is accountable for the reporting, database management, and overall effectiveness of the program and commands and/or subordinate units.

c. Work with the Immediate Superior in the Chain of Command to meet shared Cyber IT/CSWF management oversight and compliance responsibilities.

d. Ensure Service electronic reporting mechanisms are used to allow for consistent data reporting.

e. Whenever possible, the Cyber IT/CSWF-PM role shall be a primary duty. It is not required to be a new, and separate, billet or position, but shall be assigned to a person in a position within the command's Cyber IT/CSWF. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization or by the Command ISSM.

f. Be a U.S. citizen. Non U.S. citizens and contractors may not serve as Cyber IT/CSWF-PM.

13. COMMAND INFORMATION SYSTEMS SECURITY MANAGER (ISSM).

The Command ISSM (formerly known as IAM) shall:

a. Be responsible for ensuring that all cybersecurity components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

b. Be trained, qualified, and appointed in writing by the Commanders of DON organizations. Develop and maintain an organizational or system-level cybersecurity program that includes cybersecurity architecture, requirements, objectives and policies, cybersecurity personnel, and cybersecurity processes and procedures.

c. Maintain a repository for all organizational or system-level cybersecurity-related documentation.

d. Ensure that ISSOs are appointed in writing and provide oversight to ensure that they are following established cybersecurity policies and procedures.

e. Monitor compliance with cybersecurity policy and review the results of such monitoring.

f. Ensure that CSIs, tests, and reviews are scheduled, synchronized, and coordinated with affected parties and organizations.

g. Ensure implementation of IS security measures and procedures, including reporting incidents to the Commander, Command Security Manager, and appropriate reporting chains and coordinating system-level responses to unauthorized disclosures in accordance with DoD Manual 5200.01 Volume 3 for classified information or DoD Manual 5200.01 Volume 4 for Controlled Unclassified Information (CUI), respectively.

h. Ensure that the handling of possible or actual data spills of classified information resident in ISs, are conducted in accordance with reference (n).

i. Act as the primary cybersecurity advisor to the Commander for IS and PIT systems under their purview.

j. Ensure that cybersecurity-related events or configuration changes that may impact IS and PIT systems authorization or security posture are formally reported to the Commander and other affected parties.

k. Ensure the secure configuration and approval of IT below the system level (i.e., IT products and/or services) in accordance with applicable guidance prior to acceptance into or connection to a DON IS or PIT system.

l. Be military or government civilian. Non U.S. citizens and contractors may not serve as ISSM. ISSM must be appropriately cleared to DON guidance. This position will be the ISSM's primary duties at the organization (not an embedded or collateral duty).

14. COMMAND INFORMATION SYSTEM SECURITY OFFICER (ISSO).

The Command ISSO (formerly known as the IAO) shall:

a. Fulfill both the ISSM (formerly known as the IAO) and the ISSO roles when circumstances warrant. ISSOs may be military, government civilian, or contractor personnel. Non-U.S. citizens may not serve as an ISSO. ISSOs must be appropriately cleared to DON guidance.

b. Assist the ISSMs in meeting their duties and responsibilities.

c. Coordinate with the Command Security Manager to ensure that all users have the requisite security clearances and access authorization, and are aware of their cybersecurity responsibilities for DoD IS and PIT systems under their purview before being granted access to those systems.

15. PRIVILEGED USERS.

Privileged Users shall:

a. Be trained, qualified, and designated on the SAAR as a Privileged User and through completion of a PAA signed by the ISSM and validated by the Cyber IT/CSWF-PM.

b. Be appropriately cleared to DON guidance.

c. Configure and operate IT within the authorities vested in them according to DON Cybersecurity policies and procedures.

d. Notify the responsible ISSM, and when appropriate, the Command Security Manager, of any changes that might affect security posture.

e. Maintain Cyber IT/CSWF qualification as delineated in Appendix 4 of this manual, as well as maintain the required security clearance.

f. Understand individual qualification requirements of position assigned and comply with Cyber IT/CSWF requirements directed in references (a) through (f) by ensuring awareness of being personally accountable and responsible for individual development, training, and qualification compliance requirements.

g. Routinely check with their local command Cyber IT/CSWF-PM to verify his/her entry within the DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases accurately depicts his/her qualification status.

h. Be ultimately responsible for the attainment, upkeep, and maintenance of their Cyber IT/CSWF status, to include CL, qualification maintenance, and awareness of Cyber IT/CSWF policies and standards.

i. Review command PAA annually for completeness and accuracy.

16. <u>AUTHORIZED USERS</u>.

Authorized Users shall:

a. Immediately report all cybersecurity-related events (e.g., data spill) and potential threats and vulnerabilities (e.g., insider threat) to the appropriate ISSO or, in the absence of an ISSO, the ISSM and the Command Security Manager.

b. Protect authenticators commensurate with the classification of the information accessed and report any compromise or suspected compromise of an authenticator to the appropriate ISSO and the Command Security Manager.

c. Protect terminals, workstations, other input or output devices, and resident data from unauthorized access.

d. Inform the responsible ISSO when access to a particular DoD IS or PIT system is no longer required (e.g., completion of project, transfer, retirement, resignation).

e. Observe policies and procedures governing the secure operation and authorized use of DoD IT, including operations security in accordance with references (e) and (l).

f. Use DoD IT only for official and authorized purposes.

g. Prevent the unilateral bypass, strain, or test of cybersecurity mechanisms. If cybersecurity mechanisms must be bypassed, users will coordinate the procedure with the ISSO and receive written approval from the ISSM.

h. Prevent the introduction or use of software, firmware, or hardware that has not been approved by the AO or a designated representative of DoD IT.

i. Prevent relocation of or change to DoD IT equipment or the network connectivity of equipment without proper authorization.

j. Meet minimum cybersecurity awareness requirements in accordance with reference (h).

k. Complete required Derivative Classifier training prior to being granted access to a classified IT system in accordance with reference (n).

CHAPTER 3

PROCEDURES

1. CYBER IT/CS WORKFORCE STRUCTURE AND QUALIFICATIONS OVERVIEW

a. Overview

(1) As with any workforce "structure," there must be defined and repeatable processes established for the identification, tracking, and qualification of the Cyber IT/CSWF. Timely and accurate identification, tracking, and qualification of the Cyber IT/CSWF will not only be expected, but also inspected.

(2) The DON Cyber IT/CSWF structure will be based on Categories and SAs outlined in the National Initiative for Cybersecurity Education (NICE) workforce framework, as modified in the DoD Cyberspace framework and configured to meet DON requirements. The structure will also be aligned across DoD Cyberspace Lines of Operation (LOO), specifically the DoD Information networks (DoDIN), and Defensive Cyberspace Operations LOOs. (See Figure 1).

(3) The DON Cyber IT/CSWF structure includes two workforce categories as defined in reference (f), specifically the Cyber IT and CS categories. This manual does not apply to the workforce categories of cyberspace effects or intelligence (cyberspace).

(4) Additionally, the DON workforce is identified based upon the extent of their role in cyber IT and cybersecurity work. The specific workforce classifications are:

(a) Authorized User: Requires general computer skills and a baseline understanding of cybersecurity to conduct work that is not IT and/or cybersecurity focused. This is the general DON workforce - military, civilian, and contractor.

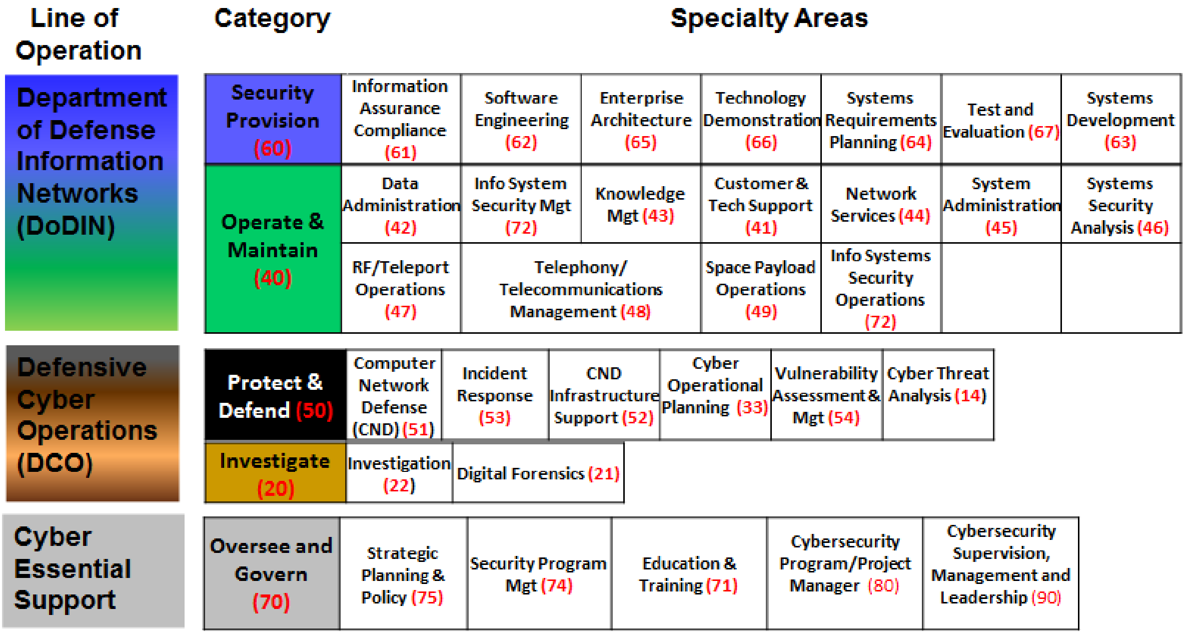
(b) Enhanced User: Authorized Users who require detailed knowledge of Cyber IT and/or cybersecurity to support work in the development, maintenance, and operations of multiple DON systems including weapons, tactical, electronic and electrical services, navigation, and engineering. These personnel require an advanced knowledge of Cyber IT/CS, but their knowledge and abilities are centered on their professional area.

(c) Core Cyber IT/CS User: Authorized Users who require KSAs in the technical and managerial aspects of Cyber IT/CS. This group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risk and protect DON networks and IS.

(5) This manual details the general cybersecurity training required for all DON authorized users and the specific qualification requirements for personnel identified as "Core" Cyber IT CSWF. The manual does not address specific training or qualification requirements for "Enhanced" users.

(6) An individual is considered qualified when he or she has met all training conditions (Appendix 4) for and completed the position On the Job Training (OJT), Personnel Qualification Standards (PQS), or JQR. This includes written designation by the appropriate command personnel. See Definitions section of this manual for definitions of Trained and Qualified.

(7) The Cyber IT/CSWF structure differs significantly from the previous Information Assurance workforce structure in that it now is based upon the actual specialties and proficiency needed based upon the work, not upon the general area and system/network size. The structure also provides the means to move to a more focused qualification regimen as outlined in reference (e). Specifically: "Civilian, military, and contracted support personnel assigned to perform cyberspace specialty area tasks must meet qualification standards established in supporting issuances." By utilizing SAs and proficiency levels, the DON will identify appropriate training, education, and certification requirements along with individual proficiency demonstration in the laboratory and on the job. This process culminates in the qualification of personnel through OJT, PQS, or JQR procedure.



Line of Operation | Category | Specialty Areas

Department of Defense Information Networks (DoDIN)

Security Provision (60): Information Assurance Compliance (61); Software Engineering (62); Enterprise Architecture (65); Technology Demonstration (66); Systems Requirements Planning (64); Test and Evaluation (67); Systems Development (63)

Operate & Maintain (40): Data Administration (42); Info System Security Mgt (72); Knowledge Mgt (43); Customer & Tech Support (41); Network Services (44); System Administration (45); Systems Security Analysis (46); RF/Teleport Operations (47); Telephony/ Telecommunications Management (48); Space Payload Operations (49); Info Systems Security Operations (72)

Defensive Cyber Operations (DCO)

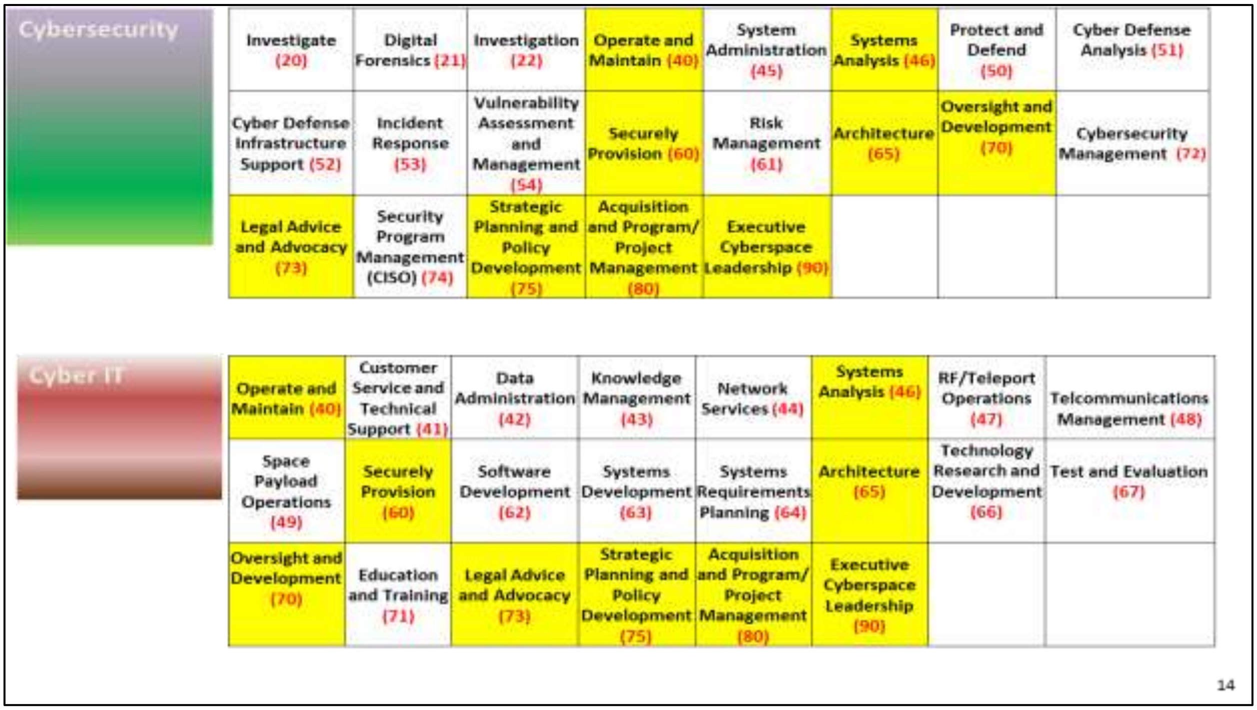
Protect & Defend (50): Computer Network Defense (CND) (51); Incident Response (53); CND Infrastructure Support (52); Cyber Operational Planning (33); Vulnerability Assessment & Mgt (54); Cyber Threat Analysis (14)

Investigate (20): Investigation (22); Digital Forensics (21)

Cyber Essential Support

Oversee and Govern (70): Strategic Planning & Policy (75); Security Program Mgt (74); Education & Training (71); Cybersecurity Program/Project Manager (80); Cybersecurity Supervision, Management and Leadership (90)

Figure 1. DON Cyber IT/CS Workforce Line of Operation Model



Cybersecurity

Investigate (20)	Digital Forensics (21)	Investigation (22)	Operate and Maintain (40)	System Administration (45)	Systems Analysis (46)	Protect and Defend (50)	Cyber Defense Analysis (51)
Cyber Defense Infrastructure Support (52)	Incident Response (53)	Vulnerability Assessment and Management (54)	Securely Provision (60)	Risk Management (61)	Architecture (65)	Oversight and Development (70)	Cybersecurity Management (72)
Legal Advice and Advocacy (73)	Security Program Management (CISO) (74)	Strategic Planning and Policy Development (75)	Acquisition and Program/ Project Management (80)	Executive Cyberspace Leadership (90)			

Cyber IT

Operate and Maintain (40)	Customer Service and Technical Support (41)	Data Administration (42)	Knowledge Management (43)	Network Services (44)	Systems Analysis (46)	RF/Teleport Operations (47)	Telcommunications Management (48)
Space Payload Operations (49)	Securely Provision (60)	Software Development (62)	Systems Development (63)	Systems Requirements Planning (64)	Architecture (65)	Technology Research and Development (66)	Test and Evaluation (67)
Oversight and Development (70)	Education and Training (71)	Legal Advice and Advocacy (73)	Strategic Planning and Policy Development (75)	Acquisition and Program/ Project Management (80)	Executive Cyberspace Leadership (90)		

14

Figure 2. DON Cyber IT/CS Workforce Category Model

(8) In order for cyber IT and cybersecurity goals to be met successfully they must have the full support and accountability of Commanders of DON organizations to achieve the following:

(a) Enforce high standards of cybersecurity governance.

(b) Treat Cyber IT/CS as a critical function that enables the unit, Command, and ultimately the DON to carry out its mission.

(c) Create culture that promotes the importance of, and embraces cybersecurity.

(d) Ensure that controls being implemented within cybersecurity are appropriate and proportionate to the risks being addressed.

(e) Stay informed and accepts ultimate responsibility and accountability.

(9) Commercial/Industry certifications will remain part of the DON Cyber IT/CSWF Strategy.

(a) The DON's Cyber IT/CSWF credentialing criteria has been expanded to allow for three different routes towards meeting qualification requirements: DoD approved baseline commercial and/or industry certification, DON approved formal Cyber IT/CSWF-related military training, or DON approved Cyber IT/CSWF-related academic degree.

(b) Depending on military enlistment or commissioning, or civilian hiring entry points into the Navy, initial training, and ultimate placement within the Cyber IT/CSWF, the options of formal military training or academic degree may not be a viable or a readily available option to meet the individual's immediate Cyber IT/CSWF credentialing needs. Similarly, existing military or civilian Cyber IT/CSWF employees may not have the opportunity to attend formal military training or off-duty academic degree programs. Commercial certifications and certificates can also be used to support training of Reserve members during monthly and annual drill periods where the length of military training programs would preclude attendance. In these cases, commercial and/or industry certification may be the best, more-convenient, or only option to fulfill the credentialing requirement of the Cyber IT/CSWF qualification.

(c) With this understanding, the DON is not distancing itself from commercial certifications, nor is the DON removing the option for commercial certification to meet Cyber IT/CSWF qualification. Commercial certification is still required for those Cyber IT/CSWF who have not met the credentialing requirement via formal military training or academic degree. For those Cyber IT/CSWF personnel who chose to, or their only option is to, hold a commercial and/or industry certification, the Cyber IT/CSWF member must earn and maintain the certification in accordance with DoD, DON, and Certification Agency requirements.

b. Cyber IT/CS Workforce Structure

(1) Commanders, COs, OIC, and Directors are ultimately responsible for the timely and accurate identification and tracking of their Cyber IT/CSWF. Identification and tracking of command Cyber IT/CSWF personnel may be delegated to the Command Cyber IT/CSWF-PM, who will:

(a) Capture new Cyber IT/CS billets within the DON Cyber IT/CSWF enterprise tracking tool (TWMS) within 3 months of billet identification (regardless of billet being filled or unfilled). Contractor records will be recorded in the personnel section of the TWMS Cyber IT/CSWF module. They will be imported from the Defense Enrollment Eligibility Reporting System (DEERS) for those with a Common Access Card (CAC) or entered locally as a new record if no CAC is assigned.

(b) Ensure cybersecurity billets (including contracted support personnel positions) are removed from the DON CSWF enterprise tracking tool (TWMS), within 3 months of billet cut (but only after billet is no longer occupied). Billet deletion must be accomplished within the appropriate manpower ADS.

(c) Track initial training, CL, and sustained qualification for all assigned Cyber IT/CSWF personnel.

(d) Validate completion of initial and annual PAA documentation/review.

(e) Validate SOW/PWS include the requirement for contracted support personnel positions to qualify (and maintain qualification) as a provision of the contract.

(f) All Cyber IT/CS Positions must be properly coded in Service manpower databases using proper procedures for the update of those databases.

(g) Validate civilian Position Description (PD), including the requirement to qualify (and maintain qualification) as a condition of employment with the following wording:

> This position has been designated as a Cyber IT/Cybersecurity Workforce position in specialty area (insert specialty area code) and as a condition of employment incumbents of the position are required to comply with the DON Cyber IT/CSWF Program requirements of SECNAV M-5239.2, which include:
>
> 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 level commensurate with the scope of major assigned duties for the position to which you are assigned, and;
>
> 2. Participate in a continuous learning program as described in SECNAVINST 1543.2. A minimum of 40 hours of Cyber IT/CSWF related continuous learning annually documented in a current individual development plan signed by both the employee and supervisor.

(2) Cyber IT/CS duties may be performed as primary or additional/embedded duty, by a DoD employee (civilian, including local nationals (LNs) or military) or by contracted support personnel (including LNs). Some cybersecurity duties are limited to military and government civilian personnel. Assignment of local and foreign nationals (FN) must be in accordance with reference (e).

(3) Personnel performing cybersecurity duties addressed in reference (b) and in this manual include those with the following cybersecurity oversight responsibilities:

(a) Work closely with data owners, IS owners, and users to ensure secure use and operation of IS and networks.

(b) Ensure rigorous application of cybersecurity policies, principles, and practices in the delivery of all information technology (IT) services.

(c) Maintain system audit functions and periodically review audit information for detection of system abuses.

(d) Identify cybersecurity requirements and actively participate as subject matter experts in the IT acquisition development process.

(e) Assess and implement identified corrections (e.g., system patches and fixes) associated with technical vulnerabilities as part of the Information Assurance Vulnerability Management Program, consistent with references (b) and (h), and reference (i).

(f) Maintain configuration control of hardware, systems, and application software.

(g) Identify and properly react to security anomalies or integrity loopholes such as system weaknesses or vulnerabilities.

(h) Install and administer user identification or authentication mechanisms.

(i) Control and monitor privileged access to DoD systems. Allow only the minimum Privileged Access required to perform specific tasks/duties on specific DoD systems. Privileged Access shall be the minimum required to accomplish/support mission requirements.

c. Cyber IT/CS Workforce Categories, Specialty Areas and Proficiency Levels.

(1) In addition to the categorization of DON Cyber IT/CSWF positions and personnel as part of the Cyber IT or the CSWF categories, this manual also includes the cyber workforce categories and SAs outlined in the NICE CSWF framework as revised and configured within the DON Cyber IT/CSWF framework. Specifically these categories and specialties are:

(a) CSWF Category. Group of common major cybersecurity functions, comprised of one or more SAs (e.g., Protect and Defend, Operate and Maintain). See reference (f).

(b) Cybersecurity SA. A Cybersecurity SA represents an area of concentrated work, or function, within cybersecurity. Included in each SA are typical tasks and KSAs. See reference (f).

(2) In addition to the categories and SAs, the DON framework also incorporates proficiency levels in order to more effectively identify qualification requirements.

(3) Personnel may obtain applicable experience when working in either the Cyber IT or Cybersecurity categories. Experience gained within each category can be combined to provide the total qualifications/experience necessary for those whose work involves tasking in both categories.

(4) The proficiency levels incorporated into the DON qualification framework include:

(a) Entry/Apprentice –Basic understanding of computer systems and related cybersecurity software and hardware components.

1. 1-3 years' experience (recommended)

2. Enlisted E-1 through E-4

3. Officer O-1 through O-2

4. Civilian Grades 5, 7, and 9

(b) Intermediate/Journeyman –Working knowledge and application of IS and security operational characteristics for a variety of computer platforms, networks, software applications, and OSs.

1. 4-6 years' experience (recommended)

2. Enlisted E-5 through E-6

3. Officer O-3 through O-4

4. Civilian Grades 9, 11, 12

(c) Expert – Advanced application and mastery of IS, plans, and functions, and is responsible for the management of complex projects, and initiatives with large scope.

1. 7+ years' experience (recommended)

2. Enlisted E-7 through E-9

3. Officer O-5 through O-6/W-1 through W-5

4. Civilian Grades 13 and above

(5) Each DON Cyber IT/CSWF position must be identified with a category, SA, and a proficiency level. Categories and SAs are shown in Figure 2.

(6) A position may require proficiency at multiple levels. In such cases, the level and related qualification requirements will be as necessary to accurately depict the capabilities and proficiencies required by the position. Individuals performing functions in multiple categories or SAs must be qualified in the appropriate SAs applicable to their position.

(7) CSWF categories, SAs, and proficiency levels may correlate directly to civilian grades, military ranks, or specific occupational classification standard.

(8) In order to create an enterprise standard, the DON has established a cybersecurity framework detailing categories and SAs.

2. CYBER IT/CS WORKFORCE QUALIFICATION OVERVIEW.

The Cyber IT/CSWFQP validates a cyber IT/CS practitioner's knowledge and understanding of facts, concepts, and principles that the DoD Cyber IT/CS community deems critical to successfully perform functions, implement programs, and pursue missions necessary to deliver cyber capabilities to the DON. The community includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risks and protect DON systems and information.

a. The Cyber IT/CSWFQP is mandatory for all Cyber IT/CS personnel who will be or are already performing Cyber IT/CS functions as a primary and/or additional duty on behalf of (and as specified by) a DON organization or are working towards qualification for assignment to a cybersecurity position. This initiative is intended to ensure that there is a common set of capabilities among Cyber IT/CS personnel that promotes interoperability, facilitates professional development and training, and develops a workforce of qualified Cyber IT/CS professionals.

b. As a condition of privileged access to any IS, personnel performing Cyber IT/CS tasks described in this manual must satisfy both preparatory (initial training) and sustaining DoD Cyber IT/CS qualifications requirements. Additionally, personnel assigned to Cyber IT/CS positions requiring privileged access must complete a PAA (see Appendix 2). DON organizations may not reduce the mandated requirements of this agreement to meet their needs; any requirements above and beyond what is provided in this manual may be executed, but at the expense of the DON organization.

c. The qualification requirements of this manual apply to DoD civilian employees, military personnel, LNs, and support contractors performing the Cyber IT/CS roles below and described in detail in paragraphs 2 through 6 of this Chapter.

d. Cyber IT/CSWFQP is intended to produce Cyber IT/CS personnel with a baseline understanding of the fundamental Cyber IT/CS principles and practices related to their assigned position. Each category, SA, and proficiency level has specific qualification requirements. Meeting these requirements will require a combination of credentialing (education, formal training, and certification), continuing education, and experience activities (OJT, PQS, or JQR). The activities (training, testing, OJT, and practice) required for qualification requirements must be provided by the DON at no cost to government employees (military or civilian).

e. The DON must use approved training, education and certifications, and JQR documented in the DON Cyber IT/CS Workforce Qualification Matrices (Appendix 4). The matrices outline minimum requirements. Organizations may identify and require additional qualification activities if appropriate.

f. Approved training, education and certifications will demonstrate close correlation to the Cyber IT/CS categories, SAs, and proficiency levels, as described in paragraphs 2 through 6 of this Chapter and demonstrate portability throughout the DoD, the Federal Government, and the private sector.

g. Individuals not meeting qualification requirements of their Cyber IT/CS position must be reassigned to other duties, consistent with applicable law. Until qualifications are attained, individuals in Cyber IT/CS positions not meeting qualification requirements may perform those duties under the direct supervision of an appropriately qualified individual unless the qualification requirement has been waived due to severe operational or personnel constraints. If the individual fails to achieve qualification within 6 months of failure to qualify or the expiration of operational or personnel constraints, they must be removed from the Cyber IT/CS position.

h. Appendix 3 establishes the criteria and process for approval of credential(s) for SAs.

i. Personnel utilizing Cyber IT/CS certification to meet Cyber IT/CS training and/or education requirements must adhere to all recertification policies set by their certification provider and ensure that their certifications stay active. This means that the certification holder must maintain the certification vice taking the exam each time the certification expires.

j. To support Cyber IT/CS professionals the DoD Information Assurance Support Environment (IASE) provides DoD cybersecurity and cybersecurity policy, training requirements, and DoD-sponsored training. The IASE is located at http://iase.disa.mil/.

k. Contractor personnel supporting Cyber IT/CS roles in paragraphs 2 through 6 of this Chapter shall obtain the appropriate DoD-approved baseline qualifications prior to specialty-related task(s). They may be provided an appropriate amount of time to complete DON position specific qualification including JQR if required. The contracting officer will ensure that contractor personnel are appropriately qualified. Additional training on local or system procedures may be provided by the DoD organization receiving services. The DoD may be required to provide qualification training to contractors when it is not reasonably available in the commercial sector or for DoD unique technology or processes.

l. Organizations employing LNs should coordinate in advance with appropriate offices, the Local or Country Human Resources section of OPM, local unions, and/or the Command Human Resources office.

3. <u>CYBER IT/CS POSITION MANAGEMENT</u>

a. <u>IDENTIFYING CYBER IT/CS POSITIONS</u>

(1) Cyber IT/CSWF positions have been identified and coded with a Cyber IT/CSWF code based upon the DON Cyberspace Workforce framework categories and SAs. Cyber IT/CSWF codes can be found at the TWMS Module (<u>https://twms.navy.mil/login.asp</u>) and at the Commander Navy Information Dominance Forces (NAVIDFOR) Cyber IT/CSWF website (https://usff.portal.navy.mil/sites/cyberfor/default.aspx?target=).

(2) Cyber IT/CSWF positions may also be assigned a DoD function code.

(3) With alignment to the NICE framework, the Cyber IT/CSWF position is what sets the qualification requirements. Once coded as Cyber IT/CS, a position may be associated with one or more SAs.

(4) The TFMMS shall contain all approved Navy Cyber IT/CSWF position information.

(5) The Marine Corps TFSMS shall contain all approved Marine Corps Cyber IT/CSWF position information.

(6) For civilians, the DON Cyber IT/CSWF code shall be included in Defense Civilian Personnel Data System (DCPDS) records and is included in PDs. The following statement must also be added to the PD "must meet qualification requirements of the specialty area assigned as delineated in Appendix 4 of SECNAV M-5239.2."

(7) For Cyber IT/CSWF Managers, position information is available through the DON Cyber IT/CSWF enterprise tracking tool (TWMS).

b. <u>DOCUMENTING NEW CYBER IT/CS POSITIONS</u>

(1) When an organization identifies a need to establish a new Cyber IT/CSWF position, or convert a current position to cybersecurity, whether newly establishing or converting from another occupation, established procedures for updating the appropriate manpower authoritative database (TFMMS or TFSMS) must be followed.

(2) Requests for new Cyber IT/CSWF positions must be validated by the organization's Cyber IT/CSWF-PM prior to submission to the manpower change process.

(3) Requests for new positions must follow the process for approval of new requests at the headquarters level.

(4) Managers will utilize the DON Cyber IT/CSWF framework to determine the category and SAs the position falls under.

(a) Managers shall use the DON Cyber IT/CSWF Framework SA if the description of the SA suffices to properly describe the position.

(b) If the SA description does not provide enough detail, managers shall utilize the tasks and KSAs detailed in the framework to determine the proper DON Cyber IT/CSWF code.

(c) All new Cyber IT/CSWF position requests shall include the DON Cyber IT/CSWF code in the proposal package to be submitted to manpower personnel.

(d) Position approval and updating of manpower databases will be accomplished by Service manpower personnel.

(e) All Cyber IT/CSWF positions must be properly coded in Service Manpower databases using established procedures for the update of those databases.

(f) If USN and/or USMC ADS do not include required Cyber IT/CSWF manpower data elements, the DON Cyber IT/CSWF enterprise tracking tool (TWMS) will be used to record and maintain the information.

c. MODIFYING CYBER IT/CSWF POSITION INFORMATION

(1) In those cases where an organization has identified a need to modify a Cyber IT/CSWF position, the established procedures for changing the authoritative manpower database (TFMMS or TFSMS) must be followed.

(2) Requests for modification of DON Cyber IT/CSWF positions must be validated by the organization's Cyber IT/CSWF-PM prior to submission to the manpower change process.

(3) Managers will utilize the DON Cyber IT/CSWF framework to determine the category and SA changes. A justification for the change must be included in any submission.

(a) Managers shall use the DON Cyber IT/CSWF Framework SA if the description of the SA suffices to properly describe the position.

(b) If the SA description does not provide enough detail, managers shall utilize the tasks and KSAs detailed in the framework to determine the proper DON Cyber IT/CSWF code.

(c) Once identified, the manager should include both the new and old DON Cyber IT/CSWF code in the proposal package to be submitted to manpower personnel.

(d) Position code change approval and updating of manpower databases will be accomplished by Service manpower personnel.

(4) If USN and/or USMC ADS do not include required Cyber IT/CSWF manpower data elements, the DON CSWF enterprise tracking tool (TWMS) will be used to record and maintain the information.

4. CYBER IT/CSWF PERSONNEL MANAGEMENT.

Personnel management includes much more than just the identification of a position and associated position related information. Personnel information exists in Navy and Marine Corps military personnel and training systems and in the DCPDS. Not all required personnel data resides in these systems, nor is it readily available to the Cyber IT/CSWF-PM from those databases. The DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases will capture and maintain military and civilian cybersecurity personnel information. DON/Navy/Marine Corps authoritative manpower, personnel and readiness databases processes are included in Appendix 5.

a. IDENTIFYING CYBER IT/CSWF PERSONNEL.

Uniformed Cyber IT/CSWF personnel remain a part of the Cyber IT/CSWF regardless of whether they are currently assigned to a Cyber IT/CSWF position. Civilian personnel are considered as part of the Cyber IT/CSWF when assigned to a Cyber IT/CSWF position. Cyber IT/CSWF personnel may be identified in the following ways:

(1) A DON Cyber IT/CSWF code and/or DoD Function is a part of their personnel record in a military personnel system or in DCPDS.

(2) An identified military code such as Military Occupation Specialty, Navy Enlisted Code, Sub Specialty Code, or Additional Qualification Designator is a part of their personnel record.

(3) They are listed as a member of the Cyber IT/CSWF with the appropriate DON Cyber IT/CSWF code in the DON/Navy/Marine Corps authoritative personnel and readiness databases.

b. <u>DOCUMENTING CYBER IT/CSWF PERSONNEL INFORMATION</u>

(1) Cyber IT/CSWF personnel information includes much more than just the designation as a member of the Cyber IT/CSWF. In addition, it includes information related to training, education, credentialing, individual qualification, continuing education, and cybersecurity team assignment information.

(2) If USN and/or USMC ADS do not include required Cyber IT/CSWF manpower data elements, the DON Cyber IT/CSWF enterprise tracking tool (TWMS) will be used to record and maintain the information.

(3) Contractor records will be recorded in the personnel section of the TWMS Cyber IT/CSWF module. They will be imported from DEERS for those with a CAC or entered locally as a new record if no CAC is assigned.

c. <u>MAINTAINING AND MODIFYING CYBER IT/CSWF PERSONNEL INFORMATION</u>

(1) The Command Cyber IT/CSWF-PM is responsible for the maintenance of Cyber IT/CSWF personnel information. The Cyber IT/CSWF-PM shall ensure the record is maintained within the DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases while personnel are assigned, a copy is included in transfer packages for personnel and follow-on organization's use, and that personnel have access to their information.

(2) Maintenance of Cyber IT/CSWF personnel information required by military personnel and training systems is maintained in those systems. For civilians, if the information is required by DCPDS it shall be maintained there. Policy regarding updating of military and civilian systems must be followed to update these systems. DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases will access this information and aggregate for the individual’s, Cyber IT/CSWF-PM and DON, USN, and USMC Cyber IT/CSWF leadership use.

(3) Information residing only in DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases will be the responsibility of the individual and the Cyber IT/CSWF-PM. Changes will be made in accordance with DON/Navy/Marine Corps authoritative personnel and readiness databases procedures outlined in Appendix 5.

(4) Cyber IT/CSWF-PMs shall review workforce information in DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases at least semi-annually and ensure that it remains current and accurate.

(5) Cyber IT/CSWF-PMS will ensure that Cyber IT/CSWF personnel data is captured in the DON Cyber IT/CSWF enterprise tracking tool (TWMS). In those cases where the information is not available from the personnel or training ADS, then the Cyber IT/CSWF-PM will enter directly into the DON Cyber IT/CSWF enterprise tracking tool (TWMS).

(6) Cyber IT/CSWF-PM(s) will report Cyber IT/CSWF metrics to DDCIO (Marine Corps) or DDCIO (Navy)/NAVIDFOR annually to meet FISMA reporting compliance.

5. <u>CYBER IT/CSWF LEARNING CONTINUUM</u>

a. <u>THE CONTINUUM</u>

(1) Cyber IT/CSWF education, training, and certification are key components in the overall qualification of the workforce. CL is the component of workforce qualification that addresses the requirements necessary to keep the workforce current. Education, training, certification, and CL will all be mapped to SAs within the framework and will be based upon the mapping of SA tasks and proficiency levels. When appropriate, associated KSAs may be used in the mapping process. Security and OS/CE education, training, and certification will be required of workforce personnel.

(2) For the DON Cyber IT/CSWFQP, academic degrees, military course completion credentials and Cyber IT/CSWF certifications may all be used to meet the knowledge requirements piece of qualification.

(3) The Cyber IT/CSWF learning continuum is based on continuous improvement throughout an individual's career. It includes both wide ranging cybersecurity and IT learning and Navy and Marine Corps service unique training.

(4) For individuals, the continuum is depicted in the requirements outlined in the DON Cyber IT/CSWF Qualification Matrix. For teams, Service Training and Readiness Manuals provide specifics.

(5) Elements of the individual learning continuum include: Military training, certification, academic degree programs, CL, on the job experience, and individual qualification programs.

(6) The DON Cyber IT/CSWFQP will be based upon credentialing, where credentials can be earned through formal certifications, educational degrees, or completion of formal military training. Other learning opportunities included in CL will be utilized to maintain credential currency. New IT training provided in conjunction with installation, if not a part of a formal military or recognized certification program, will be considered as interim until such time as it becomes part of a formal program. All education, training, and certification programs will be

included in the Cyber IT/CSWF Qualification Matrix (Appendix 4). CL opportunities will be approved in accordance with certification provider standards, academic degree requirements, and military training guidelines.

(7) All training, education, and certification programs approved for inclusion in the DON workforce qualification program will be approved through a rigorous review and approval process. International, national, and DON standards must be met prior to inclusion in the DON Cyber IT/CSWF Qualification Matrix. Vetting standards will be established by the DON Cyber IT/CSWF MOCC. Further detail is provided in Appendix 3.

b. CYBER IT/CSWF EDUCATION

(1) Cyber IT/CSWF education is collegiate-level education obtained through programs leading to an academic degree and that continuing education required to keep a degree current.

(2) Cyber IT/CSWF education may be obtained through completion of approved relevant, and approved, cybersecurity degree programs – associate, bachelors, or advanced degree.

(3) Cyber IT/CSWF education may also be obtained through completion of approved Federal and Military Service Degree programs.

(4) Approved educational programs will be identified in the Cyber IT/CSWF Qualification Matrix mapped to SAs and proficiency levels.

(5) Additional information on approval of educational programs is included in Appendix 3.

c. CYBER IT/CSWF TRAINING

(1) Training requirements are aligned to the DON Cyber IT/CSWF structure and career progression. The continuum will include provisions for Cyber IT/CSWF personnel to gain and maintain proficiency in necessary skills to perform Cyber IT/CSWF tasks.

(2) Approved training may be attained through:

(a) Formal military training/course

(b) Formal industry training

(c) Cyber IT/CSWF exercises

(2) Approved training programs will be identified in the Cyber IT/CSWF Qualification Matrix mapped to SAs and proficiency levels.

(3) Additional information on approval of training programs is included in Appendix 3.

d. CYBER IT/CSWF CERTIFICATION

(1) Certifications are typically earned from a professional society and must be renewed periodically, or may be valid for a specific period of time. Certifications are one way for organizations to credential individuals with specific skill sets; they are portable, and do not rely on one company's definition of a certain job. They can enable workforce members to stand out as having necessary professional skills and provide an impartial, third-party endorsement of an individual's professional knowledge and experience.

(2) The NICE is in the process of developing a list of applicable professional certifications. The certifications list that will be contained within the National Initiative for Cybersecurity Careers and Studies portal will support the DON Cyber IT/CSWF framework, and will assist in building a technically adept, capable cadre of Cyber IT/CS professionals to protect the department’s cyber infrastructure from foreign and domestic threats. The DoD CIO's approved list of Information Assurance/Cybersecurity certifications will serve as the baseline for certifications approved for DON personnel. These certifications will be mapped to the DON Cyber IT/CSWF Framework by SA and proficiency level.

(3) Certification will be standardized across the DON to provide the necessary consistency among military, civilian, and contractor job roles and responsibilities to ensure interoperability of all segments of the Cyber IT/CSWF.

(4) Additional certification identified as required by DON personnel will be added in accordance with approval procedures outlined in Appendix 3.

(5) Cyber IT/CSWF personnel with privileged access (military, civilian, or contractor) who use certification as a means to fulfill the “Minimum Credential” criteria within the Cyber IT/CSWF Qualification Matrix must hold a current and maintained version of the certification tied to their assigned SA.

(6) In cases where the Cyber IT/CSWF member is assigned to multiple SAs, the member must hold a current and maintained version of the certification tied to each assigned SA. Where multiple SAs have similar or equivalent certifications between them, the common or equivalent certification will be held and maintained (i.e., if Certified Information Systems Security Professional (CISSP) and Global Information Assurance Certification Security Leadership Certification appears in one of the assigned SAs, and CISSP and Certified Authorization Professional appear in the other assigned SA, the CISSP is the common certification that will need to be held and maintained).

(7) Cyber IT/CSWF personnel with privileged access (military, civilian, or contractor) who use certification as a means to fulfill the “Minimum Credential” criteria within the Qualification Matrix, and whose certification expires, will have their privileged access revoked and may not continue assigned duties within the SA. Local command Cyber IT/CSWF-PMs will have to seek a short-term waiver (less than 6 months) from the appropriate DDCIO if there is a need for the unqualified Cyber IT/CSWF personnel to continue to perform duties within the SA.

(8) Most, if not all, of the DON-approved Cyber IT/CSWF certifications have a maintenance fee requirement in order to remain current or valid. Certification agencies have various maintenance fee requirements (i.e., annual, every 3 years, only when continuing education units (CEUs) are submitted, etc.). The Cyber IT/CSWF member must ensure all maintenance fees are applied in accordance with the certification agency's maintenance fee requirements.

(9) Most, if not all, of the DON-approved Cyber IT/CSWF certifications have a CL requirement in order to remain certified. Certification agencies have various programs to describe their CL program (i.e., Continuous Education, Certification Maintenance Unit, CEU, etc.). The Cyber IT/CSWF member must hold and maintain their certification in accordance with the certification agency's CL requirements.

NOTE: All Cyber IT/CSWF individuals (military, civilian, or contractor) have a separate requirement (outside the certification agency CL requirements) to do CL because of their assignment to the DON's Cyber IT/CSWF. All Cyber IT/CSWF personnel must accomplish CL (see Continuous Learning Program (CLP) section of this manual). Cyber IT/CSWF individuals shall participate annually in 40 hours of CL activities (see Chapter 3, paragraph 5e). These CLP activities might be applicable to the certification agency's certification maintenance requirements. It will be the responsibility of the certification holder to verify the Navy's CLP activities they wish to apply towards their associated certification held to meet the certification agency's CL requirements.

(10) USN Certification Funding: The Navy's Credentials Program Office/Navy Credentialing Opportunities On-Line (COOL) (https://www.cool.navy.mil) may fund for eligible Navy (not USMC) military and DON civilian (not contractor) Cyber IT/CSWF personnel's initial certification exam and annual maintenance fees.

(a) Navy COOL can fund for initial certification exam (up to 3 Navy-funded attempts) to meet Cyber IT/CSWF SA certification requirement) and annual maintenance fees, but only for the year it is due (not in advance; not in arrears).

(b) Navy COOL cannot fund for training, study/prep materials, memberships, CL, or other non-exam fees.

(c) Requests for exam/fee funding will be handled on a first come, first served basis. Eligible CSWF personnel should take advantage of funding as soon as practicable as the program is subject to funding constraints as the year progresses. Specific details can be found on the Navy COOL website (https://www.cool.navy.mil).

(11) USMC Certification Funding: Local commands will need to coordinate with a Communication Training Center or utilize the voluntary Marine COOL program to receive a testing voucher for initial Cyber IT/CSWF exam. If the individual fails certification exam, additional funding will be arranged in accordance with local procedures. If the initial Cyber IT/CSWF exam voucher was not obtained via the Marine COOL program, ownership of the

annual maintenance fees will reside at the local command, and local commands need to develop a plan to meet certification requirements. Marine COOL will pay for annual maintenance fees if successful certification or licensing was initiated through the Marine COOL Program.

(12) Cyber IT/CSWF personnel obtaining commercial certification(s) (military, civilian, and contractor), for the purpose of Cyber IT/CSWF qualification, shall have their certification recorded in TWMS. Identification of certification specifics within TWMS will be one of the criteria required before DON payment of expenses including certification provider continuing education and/or certification maintenance fees.

(13) Certified Cyber IT/CSWF (military, civilian, and contractor) should routinely check with their local command Cyber IT/CSWF-PM to verify their entry within the DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases accurately depicts their qualification status.

(14) The local command Cyber IT/CSWF-PM may have the requirement to ensure his/her Cyber IT/CSWF personnel are qualified. However, ultimately, it is the individual Cyber IT/CSWF member's responsibility to understand the requirements to comply with Cyber IT/CSWF qualification requirements and earn/maintain their own certification. The individual Cyber IT/CSWF member must be proactive and keep appraised of changes/updates that the certification agency makes to their certification requirements. Cyber IT/CSWF personnel should not rely on the certification agency to inform them of changes.

(15) In the event the Cyber IT/CSWF fails to achieve qualification compliance, the Commander/Commanding Officer shall notify the Cyber IT/CSWF member of his/her status and any required remediation. The command shall put the member in a non-Cyber IT/CSWF position, pending review of competencies and potential to achieve qualification. If a Cyber IT/CSWF position is not available, or the command determines that the person will not be able to achieve qualification, then the employee will be subject to other action, up to and including removal.

(16) Waivers. Commands may request waivers for personnel not qualified within 6 months of assignment to cybersecurity positions. The waiver will be documented by the Cyber IT/CSWF-PM and ISSM using a memorandum for the record stating the reason for the waiver and to rectify the shortfall. Waivers will only be approved by the DDCIO (Navy) and DDCIO (Marine Corps). The waiver must be routed through the chain of command and, for Navy, must be routed through NAVIDFOR.

(17) An OS/CE credential is only required for those Cyber IT/CSWF personnel identified in the Qualification Tables as requiring an OS/CE certificate of training. These personnel will be required to complete a Navy-approved training program (i.e., completed via SkillSoft Computer Based Training (CBT), Federal Virtual Training Environment (FEDVTE), Internet-based CBT, self-study course, off-base training facility, on-base training facility/course/school, etc.). Cyber IT/CSWF member must provide certificate of completion to Cyber IT/CSWF-PM to record within DON/Navy/Marine Corps authoritative manpower,

personnel and readiness databases. Note: Cyber IT/CSWF who hold the appropriate OS/CE credential meet the requirement.

e. CYBER IT/CS CONTINUOUS LEARNING PROGRAM (CLP)

(1) The DON Cyber IT/CS CLP is structured to support the continuing professional development of the CSWF throughout their careers. The CLP will include education, training, certification, and other activities that support the sustainment and continued improvement of the capabilities of the DON Cyber IT/CSWF.

(2) The overarching goal of the CLP is to improve cyber IT and cybersecurity operations, mission effectiveness and increase readiness across the cyber domain. This program provides the vehicle for personal improvement supporting career development and specialized assignments. Depending on the nature of the organization's work, workforce responsibilities, and the stage of organizational and personal development, training needs will vary. Ideally government personnel will approach CL with focused and targeted training and education and/or technical knowledge and skills commensurate with the individual's rank/grade.

(3) Professional or career development and CL should be accomplished through a blended solution of formal classroom training, experience, and electronic media. Learning activities may range from OJT to operational exercises to accredited education in accordance with reference (o).

(4) All civilian, military, and contract support Cyber IT/CSWF personnel will participate in the CLP commensurate with their occupation, rank/grade, and position. CLP requirements are as follows:

(a) Per reference (o), Cyber IT/CSWF members shall participate annually in 40 hours of CL activities; however, if circumstances preclude 40 hours in a single year, an individual may participate in 80 hours within a 2 year period to satisfy the requirement. Additionally, hours completed in a previous year may be used to meet the following year's requirement if approved by the person's supervisor. Hours may not be carried over further than the next consecutive year.

(b) General Cyber IT/CSWF CLP activities may include, but are not limited to, training in multiple cybersecurity specialties, leadership training, program management, joint warfighting tactics, ethics, acquisition, and rotational and developmental assignments. The DON Cyber IT/CSWF CL Steering Group will identify and approve general Cyber IT/CSWF CLP materials and sources in accordance with reference (o). Additionally, commands may identify and submit CL activities through their chain of command to the Steering Group for review and approval.

(c) CL required to maintain currency of commercial certification will be defined by the certification provider. CL credits obtained in support of commercial certification maintenance or sustainment can be used to meet overall DON Cyber IT/CSWF continuous education requirements. Note: if the commercial certification requires less than 40 hours per year, the member must also obtain the difference in hours between the vendor certification requirement and the overall 40 hour DON CLP requirement by completing additional general Cyber IT/CSWF CL activities.

(d) The annual CL period start date is the beginning of the calendar year. If the CL requirement is part of a commercial Cyber IT/CSWF certification, the start date is the date identified by the certification vendor.

(5) Contractors. Unless expressly provided for in the contract with the government, all responsibility for training that is required for the contractor to maintain a specific expertise, commercial certification, or CL is the sole responsibility of the contractor employee and/or the contractor's employer.

(6) The CL methodology requires training the Cyber IT/CSWF in such a way that each member of the workforce has the latest methods skills available at his or her disposal.

(7) The primary requirement of the CL is for the DON to maintain a personnel management system (DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases) to track professional development of Cyber IT/CSWF personnel with appropriate sections available to Cyber IT/CSWF leadership, personnel managers, and the individual.

(a) Cyber IT/CSWF Leadership. Leaders shall have access to statistics about their current subordinates and subordinate units, including billets/positions assigned, qualification status, and current CL attained.

(b) Cyber IT/CSWF Personnel Managers. Personnel managers shall have access to a force management section that tracks status of overall compliance in getting mandatory qualifications, dates and currency of qualifications, and traces individuals' careers.

(c) Cyber IT/CSWF Individuals. The individual's section shows a representation of one's current SA, both by military occupational code/Civilian Series/Contractor title and also by the DON Cyber IT/CSWF framework (Appendix 4). Any SA section will show the required qualifications and job skills for that profession, as well as any already completed/current that the individual may possess. Any individual in the Cyber IT/CSWF should be able to see his or her position in the DON Cyber IT/CSWF framework, the status of his or her qualification and proficiency level within a current job, and which CL events are required to maintain currency or move to a different role.

6. CYBER IT/CSWF QUALIFICATION

a. CYBER IT/CSWFQP

(1) The Cyber IT/CSWFQP includes all elements required for a person to qualify to carry out cybersecurity work. This includes security and OS knowledge, skills, abilities, and proficiencies.

(2) The program relies on assessment of a person's ability to carry out the individual and team responsibilities of the Cyber IT/CSWF position within the command's organization. Military training programs, academic education, commercial training, and certification programs, laboratory and exercise simulation environments and OJT and practical ability demonstration all play a part in the program. Additionally, the program includes proficiency level qualification requirements so that the individual is qualified based on their ability and the requirements of the position. Proficiency levels also provide a guide to the individual and the supervisor supporting the CL element of the program.

(3) With alignment to the NICE framework, the Cyber IT/CS position is what sets the qualification requirements. Once coded as Cyber IT/CS, whoever is assigned - regardless of military, civilian, or contract support occupation - must qualify as specified in this manual for that position. If the individual holds multiple positions, multiple qualifications are required. Qualification is not solely based upon an occupation.

(4) The program is designed to be revised based upon input from field managers and Cyber IT/CSWF personnel. This program is flexible enough to take input from the field and modify existing qualification options and requirements when needed. See Appendix 3 for further details.

b. CYBER IT/CSWF QUALIFICATION REQUIREMENTS

(1) All DON Cyber IT/CSWF personnel (active duty, civilian, and contractors) are directed to obtain and maintain qualification or risk removal from the Cyber IT/CSWF position. This applies to all DON Cyber IT/CSWF personnel, regardless of military specialty, civilian job series, or contract. Cyber IT/CSWF personnel who fail to maintain qualification are a weakness in their local command's (and network) security posture. COs shall assign unqualified military and civilian personnel to a supervised status for qualification/requalification or remove unqualified personnel from their Cyber IT/CSWF position while requalification is completed. Those who fail to requalify shall be permanently removed from the Cyber IT/CSWF.

(2) Waivers: All requests for qualification/requalification waivers shall be submitted to the DDCIO (Marine Corps) or to DDCIO (Navy) (via NAVIDFOR) for review, tracking, and approval. Approved waivers will have a finite/specific end-date, expectations for actions to be taken during the waiver period, and consequences/accountability if expectations are not met by the end of the waiver period.

(3) Military and Government personnel filling Cyber IT/CSWF positions shall obtain the appropriate DON-approved baseline job qualification standards within 6 months of assignment. The Commanding Officer will ensure that military and civilian personnel are appropriately qualified. Additional training on local or system procedures may be provided by the DON organization. The DON may be required to provide qualification training to military and government personnel when it is not reasonably available in the military training pipeline or commercial sector or for DON unique technology or processes.

(4) Contractor personnel supporting cybersecurity shall obtain the appropriate DON-approved baseline job qualification standards prior to being engaged. Contractors have up to 6 months to obtain the DON SA qualifications for their position outlined in Appendix 4. The contracting officer will ensure that contracts requiring CSWF personnel contain required cybersecurity language and that the contracting organization ensures contract personnel meet qualification requirements. Additional training on local or system procedures may be provided by the DoD organization receiving services. The DON may be required to provide qualification training to contractors when it is not reasonably available in the commercial sector or for DON unique technology or processes.

(5) LNs supporting Cyber IT/CSWF functions shall be qualified in accordance with guidance in this manual. Status of Forces Agreement(s), and local or country human resource agreements and policy, including local union agreements, must be taken into account when developing and implementing the LN qualification requirements.

(6) Cyber IT/CSWF JQR is applicable to all personnel conducting Cyber IT/CS, including DoDIN Operations, Defensive Cyberspace Operations, computer network defense, system development and acquisition, risk management, and vulnerability assessments supporting the DoDIN. This applies to military, government civilian, and contract support personnel.

(7) The JQR is a compilation of the minimum knowledge and skills that an individual must demonstrate in order to qualify to stand watches or perform other specific cybersecurity tasks. The objective of Cyber IT/CSWF JQR Program is to standardize and facilitate these qualifications.

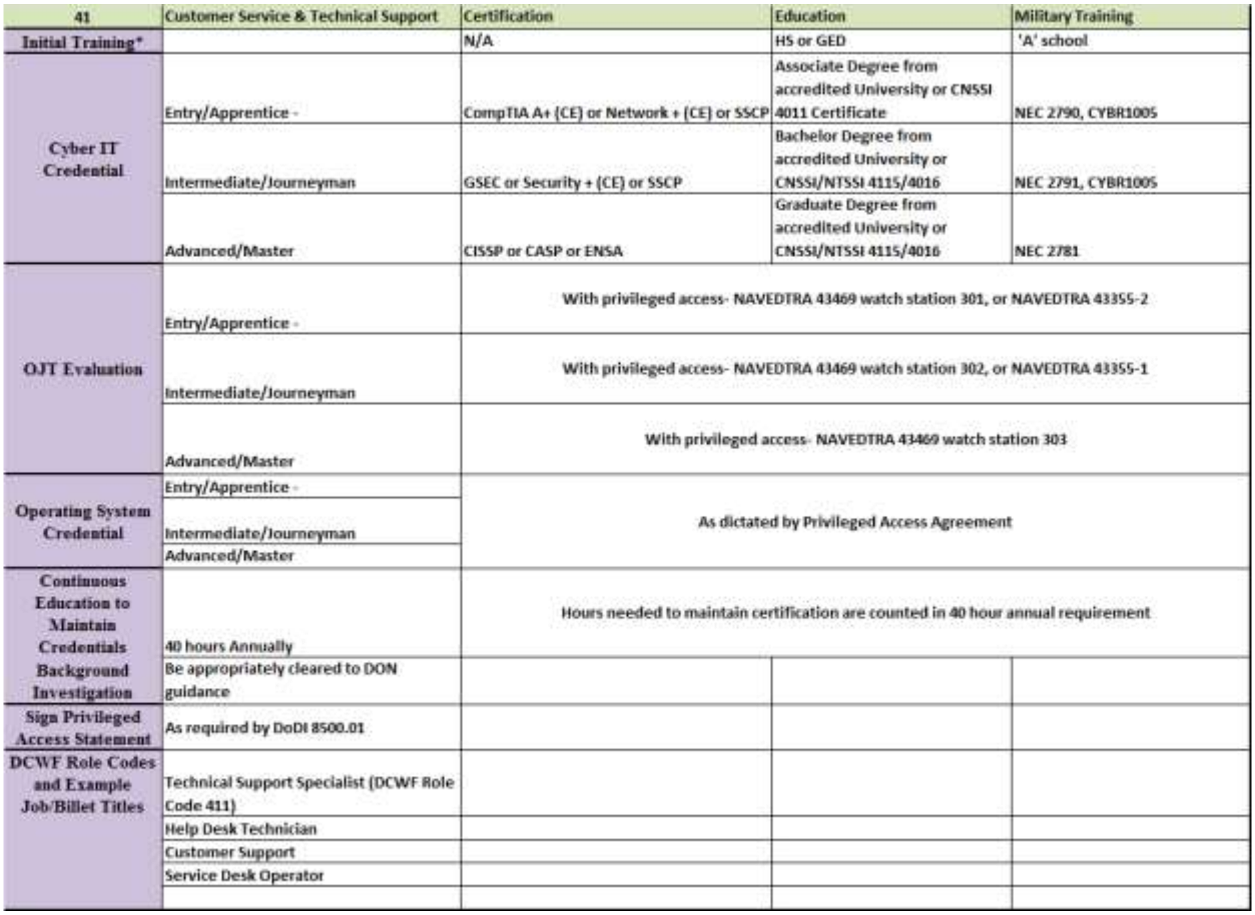
(8) The DON will develop JQR procedures to include fundamentals, systems and position/watch station requirements. The qualification procedures will address cybersecurity and OS/CE/tool requirements. Although not a part of initial qualifications, continuing education is the key element in maintaining qualification currency.

(9) Commands shall tailor qualification packages by reviewing the Service Level Qualification package by one or more qualified individuals. Commands should delete any portions covering systems and equipment not installed in their organization. Commands shall add any line items, fundamentals, systems and watch stations and/or workstations that are unique to the command but not already covered in the package. Finally, the package must be reviewed by the cognizant director/department head and required changes approved by the Commander/CO/OIC/Director or designated representative. The command will retain the approved master copy on file for use in tailoring individual packages.

(10) The Cyber IT/CSWF JQR is divided into three sections. The 100 Section (Fundamentals) contains the fundamental knowledge from technical manuals and other text necessary to satisfactorily understand the cybersecurity and OS/CE concepts and processes. The 200 Section (Systems) is designed to provide basic information on the OS/CE/Tools that will be required to be used at an organization to carry out the tasks associated with a position/watch station. The 300 Section (Watch Stations) lists the tasks required to be satisfactorily performed in order to achieve final JQR completion for a particular position/watch station.

(11) The Cyber IT/CSWF Qualification Matrix (Figure 3 below) details the Cyber IT/CSWF fundamentals and systems approved training, education and certifications by SA and proficiency level. It also details continuing education requirements.

(12) Supervisors will inform personnel as to which SA(s) and watch stations/workstations they are to qualify for and in what order.



41	Customer Service & Technical Support	Certification	Education	Military Training
Initial Training*		N/A	HS or GED	'A' school
Cyber IT Credential	Entry/Apprentice -	CompTIA A+ (CE) or Network + (CE) or SSCP	Associate Degree from accredited University or CNSSI 4011 Certificate	NEC 2790, CYBR1005
	Intermediate/Journeyman	GSEC or Security + (CE) or SSCP	Bachelor Degree from accredited University or CNSSI/NTSSI 4115/4016	NEC 2791, CYBR1005
	Advanced/Master	CISSP or CASP or ENSA	Graduate Degree from accredited University or CNSSI/NTSSI 4115/4016	NEC 2781
OJT Evaluation	Entry/Apprentice -	With privileged access- NAVEDTRA 43469 watch station 301, or NAVEDTRA 43355-2		
	Intermediate/Journeyman	With privileged access- NAVEDTRA 43469 watch station 302, or NAVEDTRA 43355-1		
	Advanced/Master	With privileged access- NAVEDTRA 43469 watch station 303		
Operating System Credential	Entry/Apprentice -	As dictated by Privileged Access Agreement		
	Intermediate/Journeyman			
	Advanced/Master			
Continuous Education to Maintain Credentials	40 hours Annually	Hours needed to maintain certification are counted in 40 hour annual requirement		
Background Investigation	Be appropriately cleared to DON guidance			
Sign Privileged Access Statement	As required by DoDI 8500.01			
DCWF Role Codes and Example Job/Billet Titles	Technical Support Specialist (DCWF Role Code 411)			
	Help Desk Technician			
	Customer Support			
	Service Desk Operator			

Figure 3 Example of Cybersecurity Workforce Qualification Matrix

7. <u>CYBER IT/CSWF COMPLIANCE</u>

a. CYBER IT/CSWF COMPLIANCE RESPONSIBILITIES

(1) The Cyber IT/CSWF mission requires knowledgeable Cyber IT/CSWF personnel to meet rapidly evolving mission areas. While other communities have their own management and training requirements, baseline Cyber IT/CSWF training, manpower and personnel tracking, and qualification requirements have been directed by Federal statute and DoD regulations and must be adhered to by Cyber IT/CSWF total force military (active and reserve), civilian (appropriated

and NAF), LNs (direct, indirect, and third-country), and contractor personnel who are charged with Cyber IT/CSWF functions as part of their Cyber IT/CSWF duties.

(2) This manual implements processes and procedures necessary to ensure compliance with the Federal and DoD regulations. It is incumbent upon the DON to comply with these processes and procedures, thereby, standardizing and improving Cyber IT/CSWF skills to ensure mission readiness.

(3) Compliance ensures the readiness and standardization (qualification baseline that all CSWF members will acquire, according to their assigned SA) of the civilian, military, and contractor Cyber IT/CSWF.

b. CYBER IT/CSWF COMPLIANCE ACTIONS

(1) The Cyber IT/CSWF compliance actions are designed to capture key information regarding the Cyber IT/CSWFQP implementation activity at the site level. Cyber IT/CSWF compliance reviews will focus on three core areas: Cyber IT/CSWF management, Cyber IT/CSWF training, and Cyber IT/CSWF qualification. Specific objectives of the Cyber IT/CSWF compliance reviews are the following:

(a) Monitor Navy and Marine Corps Cyber IT/CSWFQP implementation progress.

(b) Verify command self-reported Cyber IT/CSWFQP planning documentation and initiatives.

(c) Validate human resources management and control systems' collection of appropriate workforce data.

(d) Confirm individual Cyber IT/CSWF personnel qualification and learning plans are being utilized.

(e) Review Cyber IT/CSWF training plans and associated training budget.

(f) Ensure FISMA Cyber IT/CSWF data reported is valid.

(2) Compliance visits may be conducted by the following organizations/activities:

(a) DoD Defense Cybersecurity Program.

(b) Naval Audit Service.

(c) DON Headquarters.

(d) Service Cyber IT/CSWFQP OPRs.

(e) Inspector General.

(f) DoD, DON, USN, and USMC Command Cyber Readiness Inspection (CCRI) teams.

(3) Service OPRs are charged with ensuring commands do not receive more than one visit every 2 years, except when a reassessment is warranted.

(4) Defense Information Systems Agency (DISA), USN, and USMC provide assist visits to commands to support command program improvement, training and preparation for assessments.

8. <u>CYBER IT/CSWF PROGRAM ASSESSMENT</u>

a. All commands with Cyber IT/CSWF personnel shall include Cyber IT/CSWF management as a reportable item under reference (g). Commands shall be responsible for establishing, evaluating, and improving ICs for Cyber IT/CSWF under the MICP.

b. The command Cyber IT/CSWF Program shall be reviewed during compliance visits and other USN and USMC command visits, as appropriate.

c. NAVY CYBERSECURITY INSPECTION AND CERTIFICATION PROGRAM (CSICP). The CSICP is the Navy's process of formally inspecting shipboard Cybersecurity posture based on DoD, DON, DISA, and National Institutes of Standards and Technology standards. The shipboard CSI follows the same format and guidelines as the CCRI that DISA performs for shore commands. The CSI should be integrated into the ship's Fleet Readiness Training Plan and the Ashore Command Training Plans and is required as part of renewing the ship's network authority to operate.

d. Marine Corps CSIs are conducted in accordance with USMC policy. USMC assist teams prepare commands for CCRIs and conduct an assessment of the command's cybersecurity program's administration, training, personnel, operations, monitoring and assessment.

e. CYBER IT/CSWF AUDITS. The purpose of Cyber IT/CSWF audits is to help determine the possible consequences of risks posed by the current state of a command or unit's Cyber IT/CSWF qualifications. Audit specifics will be provided by the Navy and Marine Corps OPRs.

9. <u>AUTHORIZED USER TRAINING: GENERAL REQUIREMENTS</u>

a. The requirements for computer security awareness training have been established under the authority of reference (l).

b. All individuals with access to DON IT systems are required to receive and complete initial cybersecurity awareness training before being permitted access to the system(s). Upon completion of the training, they are required to acknowledge, in writing, their cybersecurity responsibilities.

c. All individuals must complete annual cybersecurity awareness training and acknowledge their continuing cybersecurity responsibilities.

d. Additionally, the DON will institute a DON wide cybersecurity training program for authorized users that builds upon the initial and annual refresher training. This program will include further detail on responsibilities based upon the person's position and roles. Specific detail will be provided for leadership, managers, end users and Cyber IT/CSWF personnel.

e. The DON will also include in the program a cyber-threat knowledge program that will address current and emerging threats and activities.

f. Training will also be developed to engage the workforce and to provide actions and reporting procedures for suspected cybersecurity events. This includes announcements of new and ongoing cybersecurity issues.

g. Insider threat training will be included in the cybersecurity training program.

h. The DON program will also provide cybersecurity information along with available resources for Service family members to navigate safely in cyberspace.

i. Commands will ensure that awareness training programs are established and administered by the command training officer working in conjunction with command cybersecurity personnel. Commands are encouraged to expand, as needed, the command program to include more than the DON provided training.

10. <u>ENHANCED USER TRAINING: GENERAL REQUIREMENTS</u>

a. Each Enhanced User of DON systems must meet qualification standards established in existing workforce qualification and training requirements assigned to billets and position requirements (e.g., acquisition, intelligence, communication).

b. Enhanced users should also receive additional Cyber IT/CS training as necessary to support their work. Additional Cyber IT/CS training should be included in their overall qualification program and detailed in Navy and Marine Corps guidance. Commands should also identify and provide enhanced Cyber IT/CS for these personnel based on command missions and needs.

c. Civilian, military, and contractor support personnel shall meet existing workforce qualification and training requirements (e.g., acquisition, intelligence).

d. This manual does not apply to enhanced user positions and personnel. Organizations should review the qualification matrices and where appropriate, access training detailed in the matrices in support of the enhanced workforce development.

APPENDIX 1

CYBER IT/CS PRIVILEGED USER DETERMINATION

It is the responsibility of the Command to determine whether a position requires privileged access. If the Command determines that privileged access is required then the Command will designate personnel assigned to the position as a “Privileged User.” The Command ISSM shall be included in the determination process. The designation of "Privileged User" can be assigned to personnel within either the Cyber IT Workforce or the CSWF categories.

1. A privileged user designation shall not be based on an occupational series, but rather on the tasks and authorities required to perform privileged access functions.

2. Determination of Privileged User will be based upon review of the requirement for privileged access and the authorizations that are granted to a Privileged User, specifically:

a. Determination that the tasks required to be performed by personnel assigned to the position require privileged access. All personnel assigned to positions requiring privileged access shall be designated Privileged Users.

Privileged access is defined as: *An authorized user who has access to system control, monitoring, administration, criminal investigation or compliance functions. Privileged access is granted to a user who configures and operates IT within the authorities vested in them according to DoD and DON Cybersecurity policies and procedures.*

b. Determination of the authority(s) required by Privileged Users:

(1) A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform per reference (t). Privileged Users operate IT within the authorities vested in them according to DoD and DON Cybersecurity policies and procedures. They may be granted authorization for one or more of the following purposes:

(a) Access to the control of functions of the IS/network, administration of user accounts, etc.

(b) Access to change control parameters (e.g., routing tables, path priorities, addresses) or routers, multiplexers, and other key IS/network equipment or software.

(c) The ability and authority to control and change program files, and other users’ access to data.

(d) Direct access to OS level functions that permit system controls to be bypassed or changed.

(e) Access and authority for installing, configuring, and monitoring security functions of IS/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.

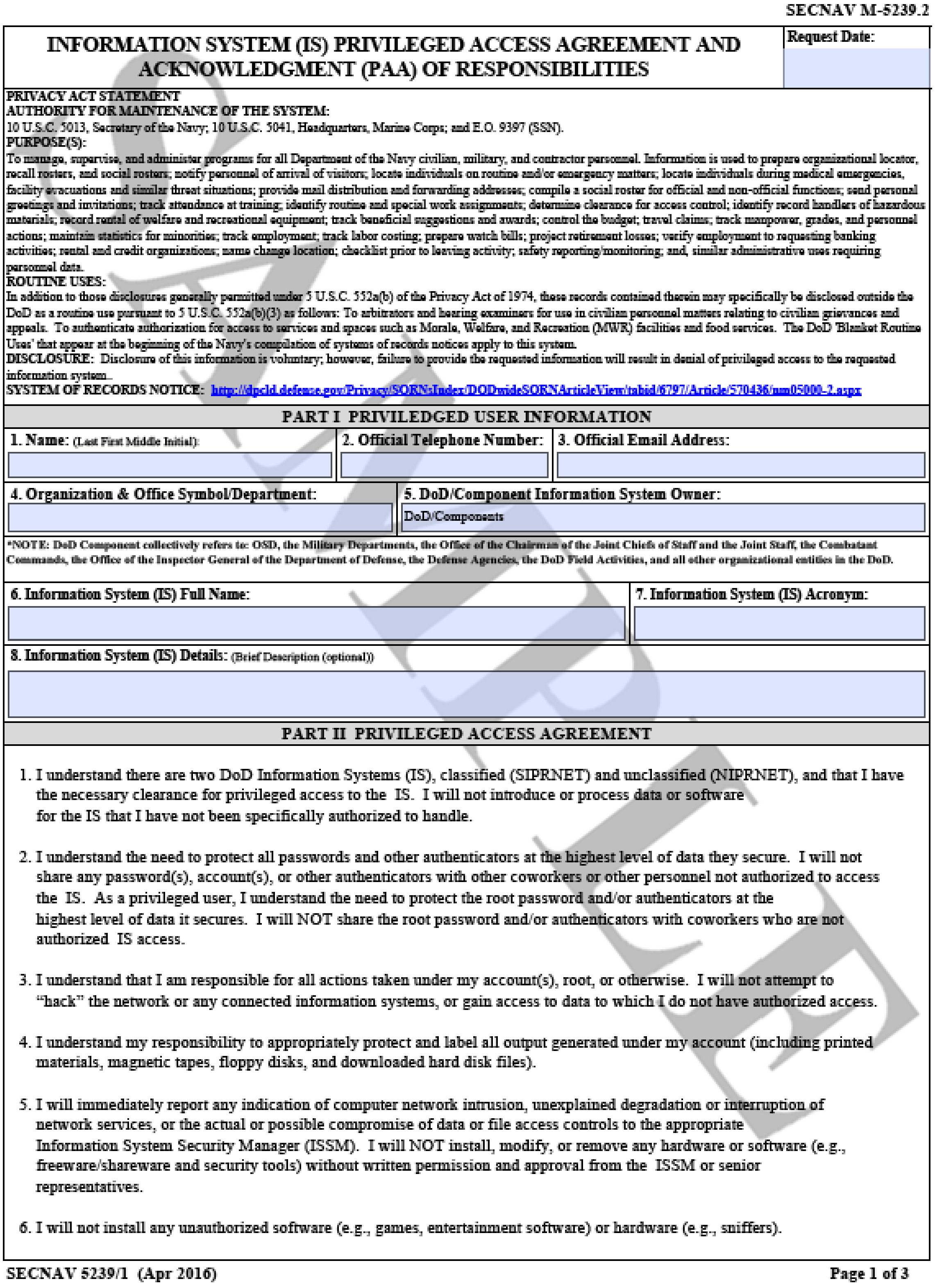
(f) Are responsible for the upkeep, configuration, and reliable and secure operation of computers, networks, and IS.

(2) Privileged User responsibilities are detailed in Chapter 1, Section 16, Privileged Users.

3. When an organization determines that the tasks associated with a position require privileged access and determines that personnel assigned to that position require specific privileged access authorities then the person shall be designated as a Privileged User and they should annotate the person's System Authorization Access Request (SAAR) form as "Privileged User", execute a Privileged Access Agreement (PAA) (Appendix 2), and determine the appropriate qualification requirements in accordance with the Matrices provided in Appendix 4. Specific Qualification requirements are based on the tasks required to be performed by personnel assigned to the position and are listed by the Cybersecurity SA in the Matrix.

APPENDIX 2

PRIVILEGED ACCESS AGREEMENT (PAA)



SECNAV M-5239.2

INFORMATION SYSTEM (IS) PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGMENT (PAA) OF RESPONSIBILITIES

Request Date:

PRIVACY ACT STATEMENT
AUTHORITY FOR MAINTENANCE OF THE SYSTEM:
10 U.S.C. 5013, Secretary of the Navy; 10 U.S.C. 5041, Headquarters, Marine Corps; and E.O. 9397 (SSN).
PURPOSE(S):
To manage, supervise, and administer programs for all Department of the Navy civilian, military, and contractor personnel. Information is used to prepare organizational locator, recall rosters, and social rosters; notify personnel of arrival of visitors; locate individuals on routine and/or emergency matters; locate individuals during medical emergencies, facility evacuations and similar threat situations; provide mail distribution and forwarding addresses; compile a social roster for official and non-official functions; send personal greetings and invitations; track attendance at training; identify routine and special work assignments; determine clearance for access control; identify record handlers of hazardous materials; record rental of welfare and recreational equipment; track beneficial suggestions and awards; control the budget; travel claims; track manpower, grades, and personnel actions; maintain statistics for minorities; track employment; track labor costing; prepare watch bills; project retirement losses; verify employment to requesting banking activities; rental and credit organizations; name change location; checklist prior to leaving activity; safety reporting/monitoring; and, similar administrative uses requiring personnel data.
ROUTINE USES:
In addition to those disclosures generally permitted under 5 U.S.C. 552a(b) of the Privacy Act of 1974, these records contained therein may specifically be disclosed outside the DoD as a routine use pursuant to 5 U.S.C. 552a(b)(3) as follows: To arbitrators and hearing examiners for use in civilian personnel matters relating to civilian grievances and appeals. To authenticate authorization for access to services and spaces such as Morale, Welfare, and Recreation (MWR) facilities and food services. The DoD 'Blanket Routine Uses' that appear at the beginning of the Navy's compilation of systems of records notices apply to this system.
DISCLOSURE: Disclosure of this information is voluntary; however, failure to provide the requested information will result in denial of privileged access to the requested information system..
SYSTEM OF RECORDS NOTICE: http://dpcld.defense.gov/Privacy/SORNsIndex/DODwideSORNArticleView/tabid/6797/Article/570436/nm05000-2.aspx

PART I PRIVILEDGED USER INFORMATION

1. Name: (Last First Middle Initial):

2. Official Telephone Number:

3. Official Email Address:

4. Organization & Office Symbol/Department:

5. DoD/Component Information System Owner:
DoD/Components

***NOTE: DoD Component collectively refers to: OSD, the Military Departments, the Office of the Chairman of the Joint Chiefs of Staff and the Joint Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the DoD.**

6. Information System (IS) Full Name:

7. Information System (IS) Acronym:

8. Information System (IS) Details: (Brief Description (optional))

PART II PRIVILEGED ACCESS AGREEMENT

1. I understand there are two DoD Information Systems (IS), classified (SIPRNET) and unclassified (NIPRNET), and that I have the necessary clearance for privileged access to the IS. I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.

2. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), account(s), or other authenticators with other coworkers or other personnel not authorized to access the IS. As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will NOT share the root password and/or authenticators with coworkers who are not authorized IS access.

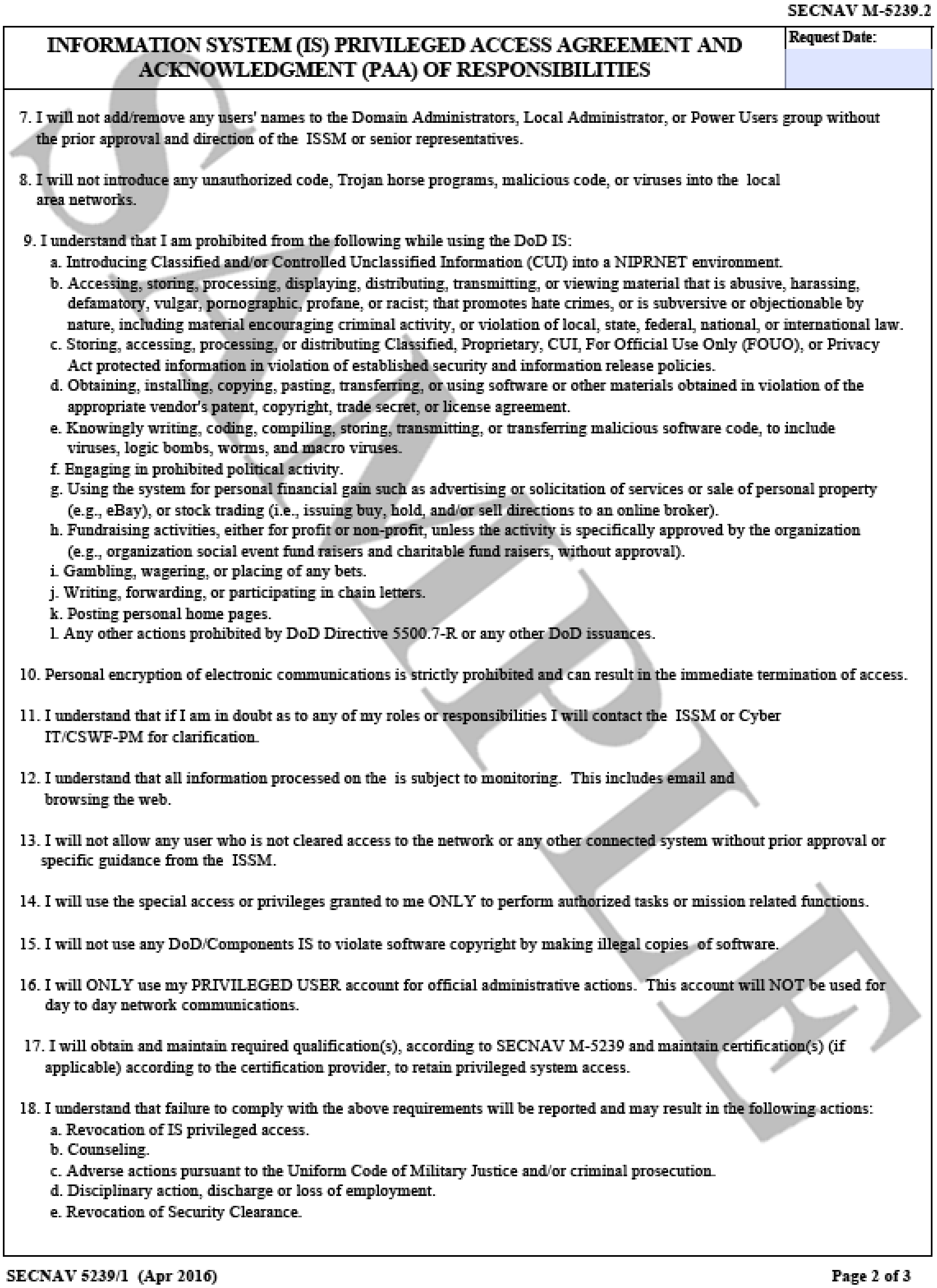
3. I understand that I am responsible for all actions taken under my account(s), root, or otherwise. I will not attempt to "hack" the network or any connected information systems, or gain access to data to which I do not have authorized access.

4. I understand my responsibility to appropriately protect and label all output generated under my account (including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files).

5. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate Information System Security Manager (ISSM). I will NOT install, modify, or remove any hardware or software (e.g., freeware/shareware and security tools) without written permission and approval from the ISSM or senior representatives.

6. I will not install any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).

SECNAV 5239/1 (Apr 2016) Page 1 of 3



SECNAV M-5239.2

INFORMATION SYSTEM (IS) PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGMENT (PAA) OF RESPONSIBILITIES

Request Date:

7. I will not add/remove any users' names to the Domain Administrators, Local Administrator, or Power Users group without the prior approval and direction of the ISSM or senior representatives.

8. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the local area networks.

9. I understand that I am prohibited from the following while using the DoD IS:
   a. Introducing Classified and/or Controlled Unclassified Information (CUI) into a NIPRNET environment.
   b. Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, state, federal, national, or international law.
   c. Storing, accessing, processing, or distributing Classified, Proprietary, CUI, For Official Use Only (FOUO), or Privacy Act protected information in violation of established security and information release policies.
   d. Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.
   e. Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.
   f. Engaging in prohibited political activity.
   g. Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold, and/or sell directions to an online broker).
   h. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers and charitable fund raisers, without approval).
   i. Gambling, wagering, or placing of any bets.
   j. Writing, forwarding, or participating in chain letters.
   k. Posting personal home pages.
   l. Any other actions prohibited by DoD Directive 5500.7-R or any other DoD issuances.

10. Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

11. I understand that if I am in doubt as to any of my roles or responsibilities I will contact the ISSM or Cyber IT/CSWF-PM for clarification.

12. I understand that all information processed on the is subject to monitoring. This includes email and browsing the web.

13. I will not allow any user who is not cleared access to the network or any other connected system without prior approval or specific guidance from the ISSM.

14. I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission related functions.

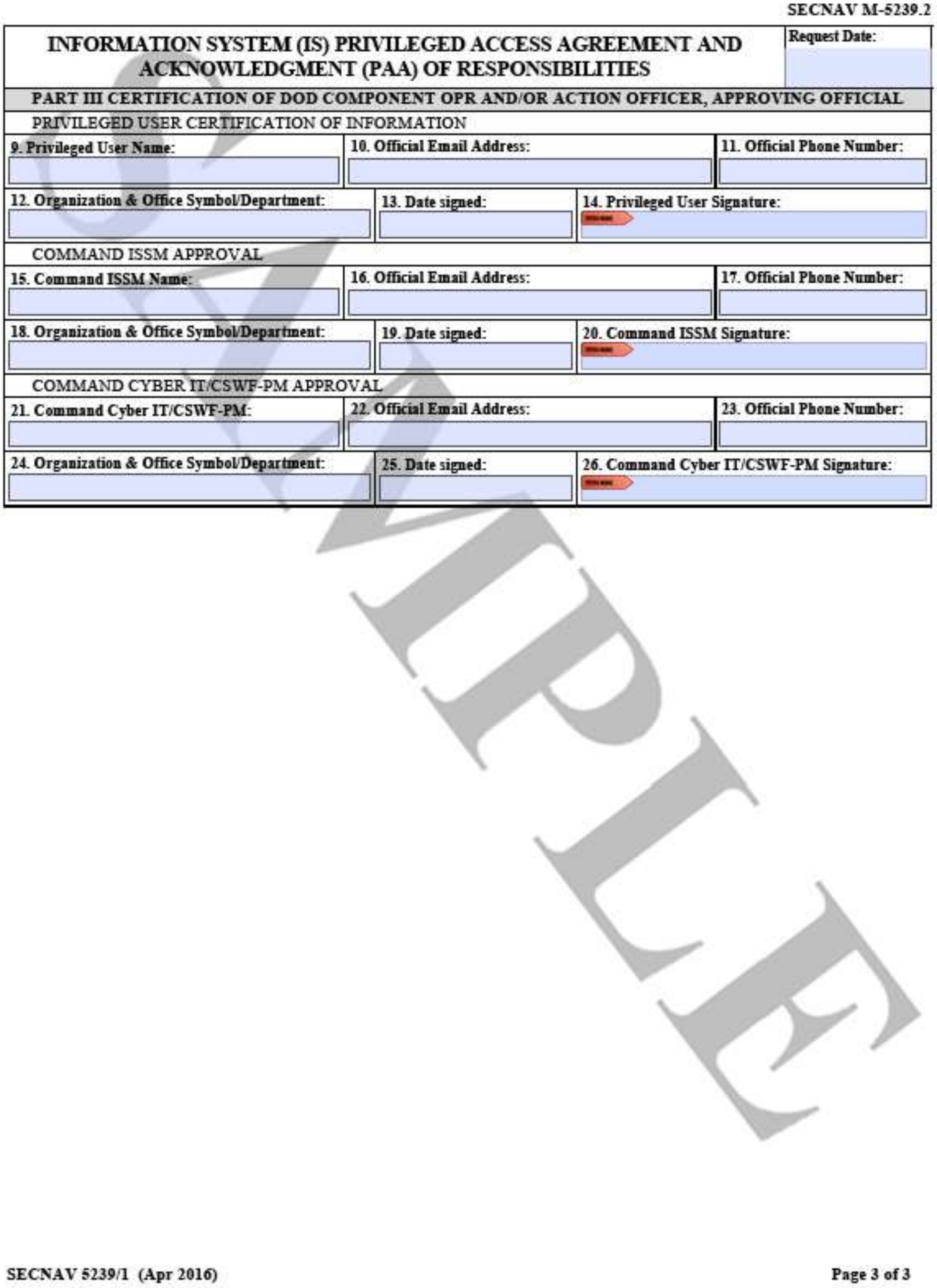
15. I will not use any DoD/Components IS to violate software copyright by making illegal copies of software.

16. I will ONLY use my PRIVILEGED USER account for official administrative actions. This account will NOT be used for day to day network communications.

17. I will obtain and maintain required qualification(s), according to SECNAV M-5239 and maintain certification(s) (if applicable) according to the certification provider, to retain privileged system access.

18. I understand that failure to comply with the above requirements will be reported and may result in the following actions:
   a. Revocation of IS privileged access.
   b. Counseling.
   c. Adverse actions pursuant to the Uniform Code of Military Justice and/or criminal prosecution.
   d. Disciplinary action, discharge or loss of employment.
   e. Revocation of Security Clearance.

SECNAV 5239/1 (Apr 2016) Page 2 of 3



SECNAV M-5239.2

INFORMATION SYSTEM (IS) PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGMENT (PAA) OF RESPONSIBILITIES		**Request Date:**
PART III CERTIFICATION OF DOD COMPONENT OPR AND/OR ACTION OFFICER, APPROVING OFFICIAL		
PRIVILEGED USER CERTIFICATION OF INFORMATION		
9. Privileged User Name:	**10. Official Email Address:**	**11. Official Phone Number:**
12. Organization & Office Symbol/Department:	**13. Date signed:**	**14. Privileged User Signature:**
COMMAND ISSM APPROVAL		
15. Command ISSM Name:	**16. Official Email Address:**	**17. Official Phone Number:**
18. Organization & Office Symbol/Department:	**19. Date signed:**	**20. Command ISSM Signature:**
COMMAND CYBER IT/CSWF-PM APPROVAL		
21. Command Cyber IT/CSWF-PM:	**22. Official Email Address:**	**23. Official Phone Number:**
24. Organization & Office Symbol/Department:	**25. Date signed:**	**26. Command Cyber IT/CSWF-PM Signature:**

SECNAV 5239/1 (Apr 2016) **Page 3 of 3**

APPENDIX 3

CYBER IT/CS TRAINING, EDUCATION, AND CERTIFICATION APPROVAL

1. The DON Cyber IT/CSWF MOCC will serve as the approval authority for education, training, and certifications included in Appendix 4, Cyber IT/CSWF Qualification Matrix.

2. The list of approved DON Cyber IT/CSWF education, training and certification credentials included in Appendix 4 must be reviewed and updated to reflect the current listing of approved training, education and certifications at least annually.

3. Any provider listed in the Cyber IT/CSWF Matrix must meet one of the following:

a. Listed as an approved and valid vendor on the General Services Administration schedule.

b. Credentialed from the National Center of Academic Excellence.

c. Approve federal agency or department training provider.

d. If Academic Institution, is accredited by a body recognized by the U.S. Department of Education or Council for Higher Academic Accreditation (CHEA).

4. Any provider listed in the Cyber IT/CSWF Matrix must confirm that the organization does each of the following:

a. Measures course(s) effectiveness;

b. Measures student review and feedback;

c. Regularly evaluates ongoing curriculum development and revision;

d. Completes evaluation(s) of the effectiveness of curriculum changes;

e. Has system capable of tracking student completion information; and

f. Delivers degree, certification, or certificate of completion.

5. DON Cyber IT/CSWF credentials may be government or commercially granted. Credentials should meet at least 80 percent of the KSAs and/or competencies identified in the SA and level for which it is identified as applicable.

a. Certifications identified and approved on the DoD list of private industry Cybersecurity and information technology certifications will serve as the baseline for commercial certification credentials for DON Cyber IT/CSWF personnel to be included in the Cyber IT/CSWF Qualification Matrix.

b. Educational Degrees. Degrees will be of a technical or management nature. Conferring institutions must be listed in the Department of Education's Database of Accredited Postsecondary Institutions and Programs and be approved by the MOCC.

c. Military Training. Training providers must be an approved federal agency or department training provider, such as Service training schools. Formal Military training will be at least 80 hours in duration to be considered for inclusion in the Cyber IT/CSWF Qualification Matrix.

6. MOCC Training, Education and Certification Advisory Team. This standing team will serve as the collection and analysis team for education, training and certification content to be included in the Cyber IT/CSWF Qualification Matrix. It will:

a. Conduct semi-annual review of the Cyber IT/CSWF Qualification matrix information.

(1) Identify potential learning gaps and identify/propose training, education and/or certifications to close gaps.

(2) Collect training education and certification content information and work with the learning provider to map to specialty area requirements.

b. Echelon II and MSC CIOs may propose additional education, training or certifications to the DON Cyber IT/CSWF MOCC via the TECAT. The proposing CIO must complete a pre-assessment of KSA coverage and submit supporting documentation to substantiate the proposed credential.

c. Compile reports recommending addition/deletion/or modification of training, education, and certifications included in the Cyber IT/CSWF Qualification Matrix.

d. Recommendations for additions or subtractions to/from the matrix must require a 70 percent vote of the standing members to be forwarded to the MOCC for approval.

Certified Information Systems Security Program	**Computer Forensics**	**Computer Networks**	**Computer Science**	**Applied Cyber Operations**
Cybersecurity Strategy and Policy	**Engineering**	**Information Technology**	**Cybersecurity/ Information Assurance**	**Information Systems Security**
Program Management	**Information Technology Management**	**Information Systems Management**	**Supply Chain Management**	**Network Management**
Software Development	**Software Applications & Programming**	**Systems and Network Auditor**	**Web Development**	**Knowledge Management**
Hard Sciences	**Mathematics**	**Risk Management**	**Operations Research**	**Space Systems**

Table 3.1 Common degree/certificate programs associated with Cyber IT/CS careers (list is not all-inclusive)

APPENDIX 4

CYBER IT/CYBERSECURITY WORKFORCE QUALIFICATION MATRIX

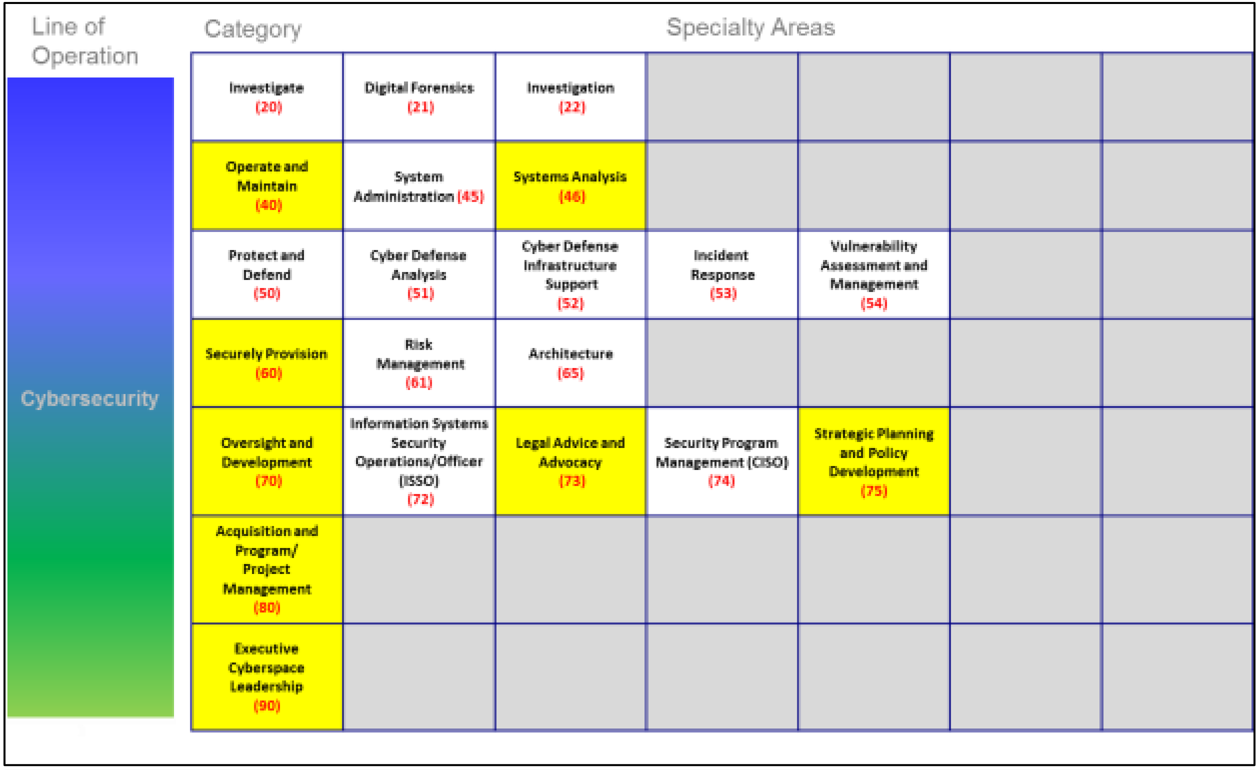
Initial Training	The training starting when a Cyber IT/CSWF member or civilian employees and contractors (when authorized) first become a member of the DON CSWF.
OJT Evaluation	With PAA = NAVEDTRA 43469 Watch Station 302 Without PAA = NAVEDTRA 43469 Watch Station 304
Continuous Learning (CL)	40 hours per year and Documented in DON Cyber IT/CSWF enterprise tracking tool (TWMS)
Privileged Access Agreement (PAA)	Signed prior to initial access and Validated annually and Revoked upon transfer or removal from Cyber IT/CSWF

Minimum Proficiency Level Assigned	Apprentice = 0 – 3 years' experience in Cyber IT/CSWF position (recommended)
	Journeyman = 4 – 6 years' experience in Cyber IT/CSWF position (recommended)
	Master = 7+ years' experience in Cyber IT/CSWF position (recommended)

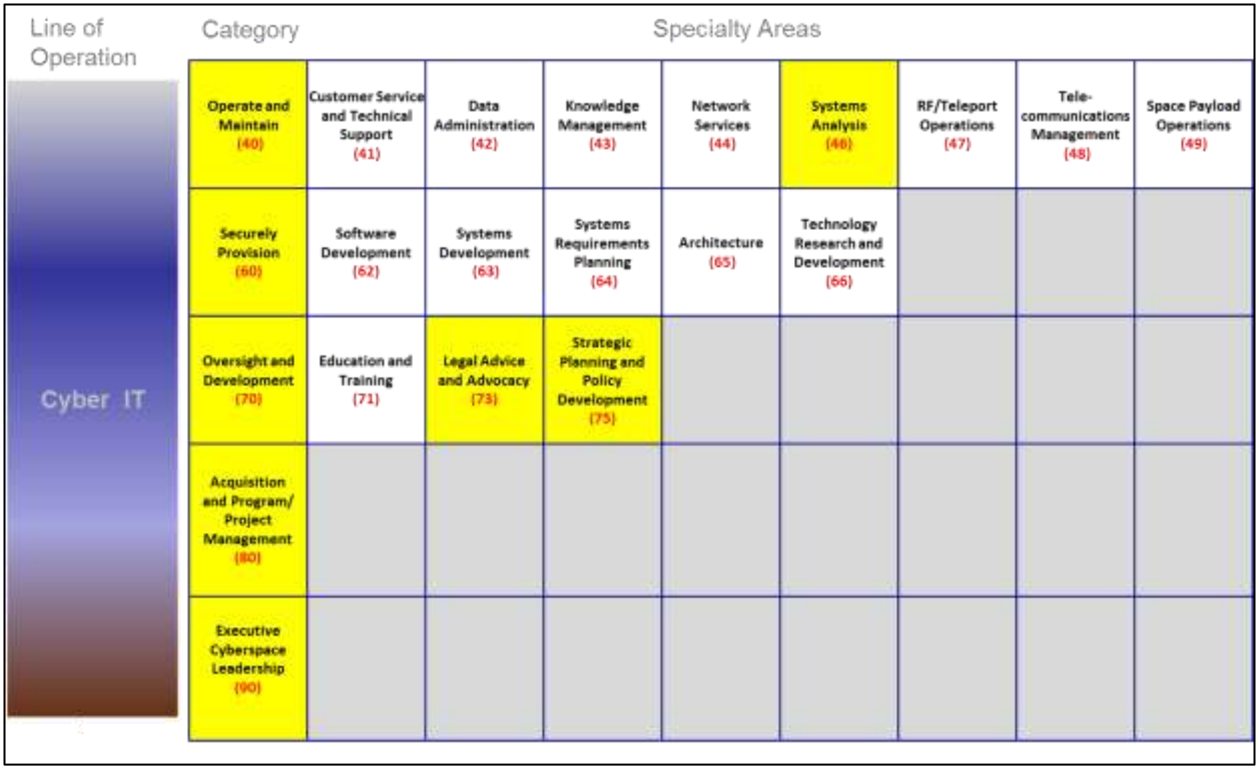
Minimum Credential	Education = DON Approved College Degree or Military Training = DON Approved Formal Military Training/Course (80 hours) or Industry Training = DON Approved Formal Industry Training/Course (80 hours or greater within last 36 months) or Industry Certification = DoD Approved Baseline Certification
OS/CE Certificate of Training	[Only applicable to specific Cyber IT/CSWF Specialty Areas] OS/CE certificate of training completion, as detailed in Qualification Matrix tables. Completed via SkillSoft CBT, FEDVTE, Internet-based CBT, self-study course, off-base training facility, on-base training facility/course/school, etc.). Cyber IT/CSWF member must provide certificate of completion to Cyber IT/CSWF-PM to record within the DON Cyber IT/CSWF enterprise tracking tool (TWMS).

EXAMPLE: Cyber IT/CSWF Qualification Matrix

NOTE: All Cyber IT/Cybersecurity Positions must be properly coded in Service Manpower databases using proper procedures for the update of those databases.



Line of Operation	Category	Specialty Areas					
Cybersecurity	Investigate (20)	Digital Forensics (21)	Investigation (22)				
	Operate and Maintain (40)	System Administration (45)	Systems Analysis (46)				
	Protect and Defend (50)	Cyber Defense Analysis (51)	Cyber Defense Infrastructure Support (52)	Incident Response (53)	Vulnerability Assessment and Management (54)		
	Securely Provision (60)	Risk Management (61)	Architecture (65)				
	Oversight and Development (70)	Information Systems Security Operations/Officer (ISSO) (72)	Legal Advice and Advocacy (73)	Security Program Management (CISO) (74)	Strategic Planning and Policy Development (75)		
	Acquisition and Program/ Project Management (80)						
	Executive Cyberspace Leadership (90)						



Line of Operation	Category	Specialty Areas							
Cyber IT	Operate and Maintain (40)	Customer Service and Technical Support (41)	Data Administration (42)	Knowledge Management (43)	Network Services (44)	Systems Analysis (46)	RF/Teleport Operations (47)	Tele-communications Management (48)	Space Payload Operations (49)
	Securely Provision (60)	Software Development (62)	Systems Development (63)	Systems Requirements Planning (64)	Architecture (65)	Technology Research and Development (66)			
	Oversight and Development (70)	Education and Training (71)	Legal Advice and Advocacy (73)	Strategic Planning and Policy Development (75)					
	Acquisition and Program/ Project Management (80)								
	Executive Cyberspace Leadership (90)								

The list of approved training, education and certifications will be posted on the Total Workforce Management Services (TWMS) Cyber IT/CSWF Module (https://twms.navy.mil). This list constitutes the approved list for the Cyber IT/CSWF as of the publication date of this manual.

Approved changes to the approved Cyber IT/CSWF Matrix will be posted on the TWMS Cyber IT/CSWF Module website. Notification of updates will be made through the Cyber IT/CSWF-PM structure and on the Cyber IT/CSWF matrix website.

APPENDIX 5

CYBER IT/CS WORKFORCE DATA MANAGEMENT

1. References (a) and (b) require that the Cyber IT/CSWF be documented and managed. DON CIO will coordinate use of the enterprise solutions to implement references (a) and (b). The enterprise tool currently used for Navy is TWMS. This tool may be utilized until an appropriate replacement is identified. USMC will also use TWMS and appropriate USMC authoritative manpower, personnel, and training systems.

2. Documentation of the Cyber IT/CSWF will be accomplished via the Cyber IT/CSWF data elements in DON/Navy/Marine Corps authoritative manpower, personnel, training and readiness databases when possible. All commands with Cyber IT/CSWF personnel are to have the command Cyber IT/CSWF-PM request access to the DON/Navy/Marine Corps authoritative manpower, personnel, training and readiness databases Cyber IT/CSWF data, as part of their assigned duties. Cyber IT/CSWF-PM will utilize TWMS, as the interim tool until DON authoritative data bases are updated to contain required data elements. Cyber IT/CSWF-PM personnel must have access to TWMS as part of their duties.

3. Data input, maintenance, validation, and verification will be accomplished by each Command Cyber IT/CSWF-PM. All commands with Cyber IT/CSWF personnel are to ensure that personnel are matched to a Cyber IT/CSWF SA. Once data has been validated, Cyber IT/CSWF management reports will be available in the system for each level of command with drill down capability within each commander's area of responsibility.

4. Cyber IT/CSWF military, government civilian, LN/FN, contractors, and non-appropriated fund personnel will be documented in the DON Cyber IT/CSWF enterprise tracking tool (TWMS) and other appropriate data bases. Personnel information will be evaluated against requirements of the position assigned in order to derive Cyber IT/CSWF readiness metrics. This is a 100% position/billet based program.

5. In order to aggregate, publish and provide consistent and reliable Cyber IT/CSWF reporting data and metrics, the DON Cyber IT/CSWF enterprise tracking tool (TWMS) must be populated and maintained. Manpower, personnel and training ADS should be integrated into the overall documentation, management and DON Cyber IT/CSWF enterprise tracking tool (TWMS) to the maximum extent possible. Only one source for each Service will be used to aggregate and publish Cyber IT/CSWF data.

6. All Cyber IT/CSWF personnel must be recorded in the appropriate DON Cyber IT/CSWF enterprise tracking tool (TWMS) within 10 business days of reporting. Following data must be recorded:

a. DON Cyber IT/CSWF Category (Cyber IT or Cybersecurity)

b. DON Cyber IT/CSWF SA (must match Billet CS SA)

c. Billet Cyber IT/CSWF SA

d. DON Workforce Cyber IT/CSWF-PM Designation Letter Issue Date (if designated as Command Cyber IT/CSWF-PM)

e. DON Workforce CS PAA complete (Yes or No)

f. DON On Waiver Expiration Date (if applicable and approved by DDCIO-Marine Corps or DDCIO-Navy via NAVIDFOR)

g. Date entered into current Cyber IT/CSWF position/billet

[NOTE: Civilians must have a current PD that states their assignment into the Cyber IT/CSWF, the requirement to qualify as a "condition of employment," and the qualification(s) expected.]

7. All Cyber IT/CSWF personnel must be recorded as "RM-Removed" in the appropriate DON Cyber IT/CSWF enterprise tracking tool (TWMS) immediately upon detachment.

8. Data base issues shall be resolved by the Command Cyber IT/CSWF-PM, Ech II/MSC Cyber IT/CSWF-PM, and the Service Cyber IT/CSWF-PM.

9. General guidelines:

a. Command Cyber IT/CSWF billets must be identified and validated (via Ech II/MSC Cyber IT/CSWF-PM).

b. Billet Cyber IT/CSWF SA and Cyber IT/CSWF Proficiency Levels for individual billets will be pre-determined and pre-populated.

c. Date reported onboard (date hired into position (civilian); date arrived at command (for military); date contract awarded (contractor)) will be recorded.

d. The following codes must be applied to Cyber IT/CSWF members, with routine alerts to the Command Cyber IT/CSWF-PM and Echelon II/MSC Cyber IT/CSWF-PM for anything other than Fully Qualified (FQ):

- **UI** - Under Instruction (e.g., recently hired/assigned personnel within their 6-month certification/qualification window). Alert to Ech II or MSC Cyber IT/CSWF-PM if UI greater than 6 months. UI cannot exceed 6 months.

- **WV** - Waivered by Higher Authority (must include end date of waiver). Alert to Echelon II or MSC if WV greater than end date.

- **RM** - Removed from the Cyber IT/CSWF (for those not meeting requirements, transferred from current command, or temporarily assigned out of the Cyber IT/CSWF duties – e.g., recruiting duty, detailed to other duties, etc…). Alert to Ech II or MSC Cyber IT/CSWF-PM on billet gap greater than 6 months.

- **FQ** – Fully Qualified (maximum duration of FQ is 3-years; all qualifications must be re-verified, at a minimum, every 3 years).

e. DON/Navy/Marine Corps authoritative manpower, personnel and readiness databases sets mandatory fields to be completed. Incomplete records are not saved (e.g., if the "cert held" field is completed, there must be a cert date and expiration date and member's cert ID, or the record is not completed and saved.)

f. DON/Navy/Marine Corps Cyber IT/CSWF personnel obtaining commercial certification(s) (military, civilian, and contractor) for the purpose of Cyber IT/CSWF qualification shall have their certifications recorded in TWMS. Identification of certification specifics within TWMS will be one of the criteria required before DON payment of continuing education and/or certification maintenance fees.

g. DON/Navy/Marine Corps authoritative manpower, personnel and readiness databases must have the capability to establish, record, and track Continuing Education or CL. Until that capability is available, CL will be recorded in TWMS. Continuous education and/or CL can also be managed within an IDP or similar personnel training event tracker.

h. Any changes in DON/Navy/Marine Corps authoritative manpower, personnel, and readiness databases that affect approved Cyber IT/CSWF billets will be flagged for Ech II or MSC Cyber IT/CSWF-PM review.

APPENDIX 6

INDIVIDUAL DEVELOPMENT PLAN (IDP)

1. **Requirement.** DoDI 1400.25, Volume 410 (DoD Civilian Personnel Management System (Reference (q)): Training, Education, and Professional Development) mandates that all DoD civilians have an Individual Development Plan (IDP).

2. **Overview.** An IDP is used to identify learning and training needs, assess professional strengths and weaknesses, and budget the resources required to meet developmental goals. The IDP serves as a tool to help develop talent, expand employees' capabilities and over a period of time, build successful careers. Designed to promote more holistic thinking, the IDP is viewed as an investment strategy that helps sustain personal and career growth while inspiring progress toward career goals.

3. **What is an IDP?** An IDP is defined as a written document used to help employees plan and chart their aspirations for career development that extends beyond their current needs and roles. The IDP provides the employee an opportunity to identify career objectives and knowledge, skills, and abilities (KSAs) needed to be successful in his/her career. It is a tool used to aid an employee and the supervisor in creating a plan to support the individual's and the command's needs:

a. Introduce short to long-term goals, assess strengths and weaknesses and plan more effectively for accomplishing career goals

b. Identify training and learning needs

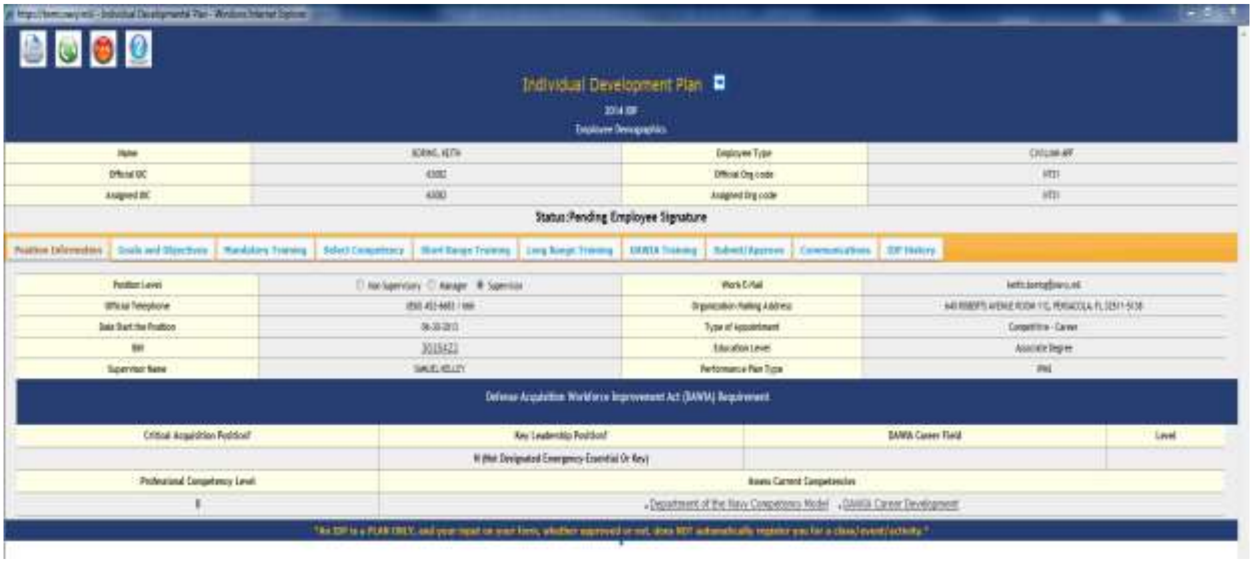
c. Improve job performance and enhance career opportunities

d. Increase KSAs

e. Serve as a documented record and a developmental agreement for recording any agreed upon developmental activities and other plans

f. Coordinate and document planned training, education and other related developmental experiences and assist in budgeting and scheduling resources

4. **Tools Needed:** Individual Developmental Plan Template (see TWMS example below).



https://twms.navy.mil/ - Individual Development Plan - Windows Internet Explorer

Individual Development Plan

2014 IDP

Employee Demographics

Name	BORING, KEITH	Employee Type	CIVILIAN APF
Official UIC	63002	Official Org code	HT31
Assigned UIC	63002	Assigned Org code	HT31

Status:Pending Employee Signature

Position Level	○ Non Supervisory ○ Manager ● Supervisor	Work E-Mail	keith.boring@navy.mil
Official Telephone	(850) 452-6683 / 666	Organization Mailing Address	640 ROBERTS AVENUE ROOM 11G, PENSACOLA, FL 32511-5138
Date Start the Position	06-30-2013	Type of Appointment	Competitive - Career
BIN	3015423	Education Level	Associate Degree
Supervisor Name	SAMUEL KELLEY	Performance Plan Type	IPMS

Defense Acquisition Workforce Improvement Act (DAWIA) Requirement

Critical Acquisition Position?	Key Leadership Position?	DAWIA Career Field	Level
	N (Not Designated Emergency-Essential Or Key)		

Professional Competency Level	Assess Current Competencies
II	• Department of the Navy Competency Model • DAWIA Career Development

"An IDP is a PLAN ONLY, and your input on your form, whether approved or not, does NOT automatically register you for a class/event/activity."

Example 1: Total Workforce Management Services (TWMS) IDP Template
https://twms.navy.mil/selfservice/

GLOSSARY

PART I. ABBREVIATIONS AND ACRONYMS

ADS	Authoritative Data Source
AO	Authorizing Official
ASN (M&RA)	Assistant Secretary of the Navy, Manpower & Reserve Affairs
CAC	Common Access Card
CBT	Computer Based Training
CCRI	Command Cyber Readiness Inspection
CE	Computing Environment
CEU	Continuing Education Units
CFR	Code of Federal Regulations
CI	Counter Intelligence
CIO	Chief Information Officer
CISSP	Certified Information Systems Security Professional
CL	Continuous Learning
CLP	Continuous Learning Program
CMC	Commandant of the Marine Corps
CNO	Chief of Naval Operations
CNSSI	Committee on National Security Systems Instruction
Command IO	Command Information Officer/Office
CO	Commanding Officer
COOL	Credentialing Opportunities On-Line
CS	Cybersecurity
CSI	Cybersecurity Inspection
CSICP	Cybersecurity Inspection and Certification Program
Cyber IT/CSWF	Cyber IT/Cybersecurity Workforce
Cyber IT/CSWF-PM	Cyber IT/Cybersecurity Workforce Program Manager
Cyber IT/CSWFQP	Cyber IT/Cybersecurity Workforce Qualification Program
CSWF	Cybersecurity Workforce
CUI	Controlled Unclassified Information
DCPDS	Defense Civilian Personnel Data System
DDCIO	Department of the Navy Deputy Chief Information Officer
DEERS	Defense Enrollment Eligibility Reporting System
DFARS	Defense Federal Acquisition Regulations System
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	DoD Directive
DoDI	DoD Instruction
DoDM	DoD Manual
DoDIN	Department of Defense Information Networks
DON	Department of the Navy
DON CIO	Department of the Navy Chief Information Officer
Ech II	Echelon II
FEDVTE	Federal Virtual Training Environment

FISMA	Federal Information Security Management Act
FN	Foreign National
FQ	Fully Qualified
HSPD	Homeland Security Presidential Directive
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IASE	Information Assurance Support Environment
IC	Internal Control
IDP	Individual Development Plan
IO	Information Owner
IS	Information System
ISO	Information System Owner
ISSM	Information Systems Security Manager
ISSO	Information System Security Officer
IT	Information Technology
JER	Joint Ethics Regulation
JP	Joint Publication
JQR	Job Qualification Requirements
KSA	Knowledge, Skills, and Abilities
LN	Local National
LOO	Lines of Operation
MAU	Major Assessable Unit
MIC	Managers' Internal Control
MICP	Managers' Internal Control Program
MOCC	Management, Oversight, and Compliance Council
MSC	Major Subordinate Commands
NAVEDTRA	Navy Education and Training
NAVIDFOR	Commander Navy Information Dominance Forces
NICE	National Initiative for Cybersecurity Education
NIPRNet	Non-secure Internet Protocol (IP) Router Network
NSPD	National Security Presidential Directive
OIC	Officer In Charge
OJT	On the Job Training
OPM	Office of Personnel Management
OPR	Office of Primary Responsibility
OPSEC	Operations Security
OS	Operating System
OS/CE	Operating System/Computing Environment
PAA	Privileged Access Agreement
PD	Position Description
PIT	Platform Information Technology
PM	Program Manager
PQS	Personnel Qualification Standards
PWS	Performance Work Statement
RM	Removed

RMF	Risk Management Framework
SA	Specialty Area
SAAR	System Authorization Access Request
SECNAV	Secretary of the Navy
SECNAVINST	Secretary of the Navy Instruction
SIPRNet	Secure Internet Protocol (IP) Router Network
SISO	Senior Information Security Officer
SM	System Manager
SOW	Statement of Work
TFMMS	Total Force Manpower Management System
TFSMS	Total Force Structure Management System
TWMS	Total Workforce Management Services
U.S.	United States
U.S.C.	United States Code
UI	Under Instruction
USN	United States Navy
USMC	United States Marine Corps
WV	Waivered
XO	Executive Officer

PART II. DEFINITIONS

Authoritative Data Source (ADS). A recognized or official data production source with a designated mission statement or source/product to publish reliable and accurate data for subsequent use by customers. An authoritative data source may be the functional combination of multiple, separate data sources (See reference (r)).

Authorizing Official (AO). (Formerly known as Principal Accrediting Authority) Responsible for authorizing the system's operation based on achieving and maintaining an acceptable risk posture.

Authorized User. Any appropriately cleared individual with a requirement to access a DoD IS for performing or assisting in a lawful and authorized governmental function. This is the general DON workforce - military, civilian, and contractor.

Basic Skill. A developed capacity that facilitates learning or the more rapid acquisition of new knowledge, or facilitates conveying information to others.

Certification. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval based on a set of standards for specific profession or occupations' functional job levels. Each certification is designed to stand on its own, and represents a certified individual's mastery of a particular set of knowledge and skills.

Command Information Officer (Command IO). The Command IO is the principal advisor to the Commander for issues regarding IM and alignment of IT investments to business priorities and assigned mission.

Community Management. Encompasses all processes required to shape the workforce to meet the service mission. Includes recruiting goals, retention monitoring, re-enlistment incentives, advancement/career progression, rotation policy and transfer to Fleet Reserve/retirement authority. CSWF Management encompasses officers, enlisted, and civilians that may be in other functional communities.

Competency. Competencies are measurable knowledge, skills, abilities, behaviors and other characteristics an individual needs to perform a particular job or job function successfully.

Core Cyber IT/CS User. Authorized users who require extensive knowledge, skill, and ability in the technical and managerial aspects of Cyber IT/CS. This group is focused on delivering cyber capabilities to the DON and includes those who design, develop, operate, maintain, and defend data, networks, network centric capabilities, computing capabilities, and communications. It also includes personnel who manage risk and protect DON networks and information systems.

Cybersecurity. Measures taken for the prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communication, including information contained therein, to ensure its availability, integrity, authentication, confidentiality, and nonrepudiation (See references (f) and (s)).

Cybersecurity Category. Group of common major cybersecurity functions, comprised of one or more specialty areas (e.g., Protect and Defend, Operate and Maintain) (See reference (s)).

Cybersecurity Specialty Area. A Cybersecurity Specialty area represents an area of concentrated work, or function, within cybersecurity. Included in each SA is typical tasks and knowledge, skills, and abilities (KSAs) (See reference (s)).

Cybersecurity Workforce (CSWF). Personnel who secure, defend, and preserve data, networks, 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.

Cyber IT/Cybersecurity Workforce Program Manager (Cyber IT/CSWF-PM). The Cyber IT/CSWF-PM is responsible for the administration of organization's CSWF Program. For small commands, the functions of the Cyber IT/CSWF-PM may be performed by a higher level organization.

Cyberspace. A global domain within the information environment consisting of the interdependent network of information technology infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. Reference (s).

Cyberspace Defense. Actions normally created within DoD cyberspace for securing, operating, and defending the DoD information networks. Specific actions include protect, detect, characterize, counter, and mitigate.

Cyberspace Effects Workforce. Personnel who plan, support, and execute cyberspace capabilities where the primary purpose is to externally defend or conduct force projection in or through cyberspace.

Cyberspace Information Technology 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.

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 the Intelligence workforces.

Cyberspace Workforce Category. The Cyberspace Workforce is composed of four categories: 1) Cyberspace Information Technology (Cyber IT), 2) Cybersecurity (CS), 3) Cyberspace Effects, and 4) Intelligence Workforce (Cyberspace).

Defense Civilian Personnel Data System (DCPDS). The DCPDS is a human resources transaction and information system that supports civilian personnel operations in the DoD. The DCPDS is designed to support appropriated fund, non-appropriated fund, and local national human resources operations. DCPDS data elements shall be used to document and track civilian personnel information in support of requirements of this Directive.

DoD Information. Any information that has not been cleared for public release in accordance with DoD policy and that has been collected, developed, received, transmitted, used, or stored by DoD, or by a non-DoD entity in support of an official DoD activity.

DoD Information System (IS). DoD-owned IS and DoD-controlled IS. A type of DoD IT.

DoD Information Technology (IT). DoD-owned IT and DoD-controlled IT. DoD IT includes IS, PIT, IT services, and IT products.

DON Senior Information Security Officer (SISO). (Formerly known as the senior Information Assurance (IA) Officer) Have authority and responsibility for security controls assessment and must establish and manage a coordinated security assessment process for information technologies governed by the DON Cybersecurity Program.

Enhanced User. Authorized users who require more detailed knowledge of Cyber IT/CS in support of work in the development, maintenance, and operations of multiple DON systems including weapons, tactical, electronic and electrical services, navigation, and engineering. These personnel require an advanced knowledge of Cyber IT/CS, but their knowledge and abilities are centered on their professional area.

Enterprise Solution (Tool). The enterprise tool currently used for Navy is the Total Workforce Management Services (TWMS). This tool may be utilized until an appropriate replacement is identified.

Functions. The specific Cybersecurity job requirements associated with a category and specialty area. The categories provide a means to distinguish between different components of work. The specialties indicate the roles that an employee performs or occupational requirements to successfully perform at different capacities of the CSWF. This approach also encourages a broader, more integrated means of identifying what an employee must know to perform the tasks that comprise a Cybersecurity position across the entire DON.

Information Owner. Official with statutory or operational authority for specified information and responsibility for establishing the controls for its generation, classification, collection, processing, dissemination, and disposal.

Information System (IS). A discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

Note: Information systems also include specialized systems such as industrial/process controls systems, telephone switching and private branch exchange systems, and environmental control systems (See reference (t)).

Information Systems Security Manager (ISSM). (Formerly known as IAM) Responsible for ensuring that all cybersecurity components have completed the appropriate evaluation and configuration processes prior to incorporation into or connection to an IS or PIT system.

Information System Security Officer (ISSO). (Formerly known as IA Officers (IAO)) Assists the ISSMs in meeting their duties and responsibilities; implements and enforces all cybersecurity policies and procedures; ensures that all users have the requisite security clearances and access authorization; initiates protective or corrective measures when a cybersecurity incident or vulnerability is discovered; and ensures that all DoD IS cybersecurity-related documentation is current and accessible to properly authorized individuals.

Intelligence Workforce (Cyberspace). Personnel who collect, process, analyze, and disseminate information from all sources of intelligence on foreign actors' cyber programs, intentions, capabilities, research and development, and operational activities.

Lines of Operation (LOO). A line that defines the directional orientation of a force in time and space in relation to the enemy and links the force with its base of operations and objectives. A LOO describes the linkage of various actions on nodes and/or decisive points with an operational or strategic objective. For the cyber domain, Cybercom has three lines of operation — DoD network operations, defensive cyber operations, and offensive cyber operations.

Local National (LN) Personnel. Civilian personnel, whether paid from appropriated or non-appropriated funds, employed or utilized by U.S. Forces in a foreign country who are nationals or non-U.S. citizen residents of that country. LNs supporting cybersecurity functions shall be qualified in accordance with guidance in this manual. Status of Forces Agreement(s), and local or country human resource agreements and policy, including local union agreements, must be taken into account when developing and implementing the LN qualification requirements.

Managers' Internal Control Program (MICP). The full scope of management responsibilities as defined in this instruction. These responsibilities include the development of effective Internal Controls (ICs) in key mission critical processes, the evaluation of ICs and correction of control deficiencies, the use of effective follow-up procedures, and the documentation and reporting requirements of this guidance. A MICP is not intended to be a stand-alone program, but rather incorporated into an organization's daily activities.

Personnel Qualification System (PQS). PQS is a qualification process for officer, enlisted, government civilians, and contract civilian personnel and is used when certification to a minimum level of competency is required prior to qualifying to perform specific duties.

Platform IT (PIT). IT, both hardware and software, which is physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems.

Platform IT (PIT) System. A collection of PIT within an identified boundary under the control of a single authority and security policy. The systems may be structured by physical proximity or by function, independent of location.

Privileged Access. An authorized user who has access to system control, monitoring, administration, criminal investigation or compliance functions. Privileged access is granted to a user who configures and operates IT within the authorities vested in them according to DON Cybersecurity policies and procedures.

Privileged User. A user that is authorized (and, therefore, trusted) to perform security-relevant functions that ordinary users are not authorized to perform (See reference (t)). Privileged Users operate IT within the authorities vested in them according to DON Cybersecurity policies and procedures, and usually has the following system controls:

- Access to the control functions of the IS/network, administration of user accounts, etc.
- Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key IS/network equipment or software.
- Ability and authority to control and change program files, and other users' access to data.
- Direct access to OS level functions that permit system controls to be bypassed or changed.
- Access and authority for installing, configuring, and monitoring security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.
- Responsible for the upkeep, configuration, and reliable and secure operation of computers, networks, and information systems.

Proficiency. Ability to perform a specific behavior (e.g., task, learning objective) to the established performance standard in order to demonstrate mastery of the behavior. CSWF personnel follow a training progression that supports continual skill development through individual and team proficiency. No one can expect to be fully qualified, proficient, or knowledgeable until they experience a variety of real life situations. Therefore, training must be developed to ensure CSWF professionals can grow and continue to meet the cybersecurity mission.

Qualified. An individual is considered qualified when he or she has met all of the conditions for "Trained" and completed the position relation On the Job Training (OJT) and Job Qualification Requirements (JQR). This includes written designation by the appropriate command personnel.

System Administrator. Individual responsible for the installation and maintenance of an IS, providing effective IS utilization, adequate security parameters, and sound implementation of established CS policy and procedures.

Trained. An individual is considered trained when he or she has completed all required foundation security, technical training, and minimum credential applicable to their position as detailed in the Cyberspace Workforce Qualification Matrix (Appendix 4).

Training

- Resident: Instructor-led in-class instruction.
- Distributive: Computer-based training via web site, computer disk, or other electronic media.
- Blended: A combination of instructor-led and distributive media. This may also include instructor-led via distributive multi-media.
- On the Job Training: Supervised hands-on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.