



Headquarters Marine Corps

Command, Control,
Communications, and Computers (C4)
Cybersecurity Division



United States Marine Corps Enterprise Cyber Security Directive

*024 Cybersecurity Workforce
Improvement Program (CWIP)
Version 1.0*

15 June 2014

FOR OFFICIAL USE ONLY

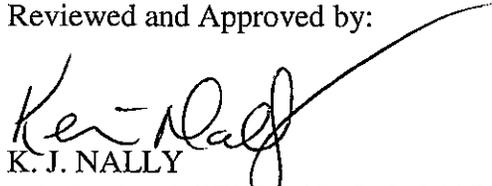
This page intentionally left blank

FOREWORD

The Marine Corps Senior Information Assurance Official (SIAO) issues Marine Corps Enterprise Cyber Security Directives (ECSDs) that guide the implementation of policy direction established in Marine Corps Order (MCO) 5239.2A, Marine Corps Cybersecurity Program (MCCSP). The modules provide procedural, technical, administrative, and supplemental guidance for all information systems used in the automatic acquisition, storage, manipulation, management, movement, control, display, switching, interchange, transmission, or receipt of data within the Marine Corps Enterprise Network (MCEN) as well as other Marine Corps information systems. Each module focuses on a distinct subject and describes a standard methodology for planning, implementing, and executing an element of the MCCSP. The Marine Corps ECSD series will be the authoritative source for implementation of Cybersecurity policy direction.

ECSD 024, Cybersecurity Workforce Improvement Program (CWIP), Version 1.0, addresses the qualification requirements for all Marine Corps Cybersecurity Workforce (CSWF) personnel.

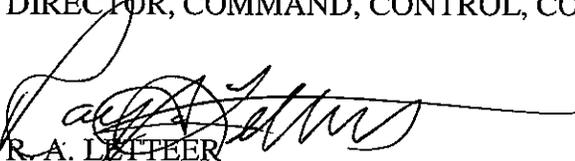
Reviewed and Approved by:



K. J. NALLY

BRIGADIER GENERAL, U.S. MARINE CORPS

DIRECTOR, COMMAND, CONTROL, COMMUNICATIONS, AND COMPUTERS



R. A. LETTEER

MARINE CORPS AUTHORIZING OFFICIAL

DIRECTOR, CYBERSECURITY DIVISION, COMMAND, CONTROL,
COMMUNICATIONS, AND COMPUTERS

DOCUMENT CONFIGURATION CONTROL

| Version | Release Date | Summary of Changes |
|----------------|---------------------|---|
| Version 0.1 | 21 Apr 2011 | Initial Draft |
| Version 0.5 | 15 June 2013 | Updated capturing updated DoD, DON and USMC Policy and Guidance |
| Version 0.8 | 2 August 2013 | Updated CRM from MCATS Feedback |
| Version 1.0 | 30 June 2014 | Updated directive draft with comment matrices input from MCATS Feedback. Released final draft revision for publication. |

Table of Contents

| | |
|---|-------------|
| EXECUTIVE SUMMARY | viii |
| SECTION 1.0: INTRODUCTION | 2 |
| 1.1 Background | 2 |
| 1.2 Purpose | 2 |
| 1.3 Applicability and Scope | 3 |
| 1.4 Cancellation..... | 4 |
| 1.5 Distribution | 4 |
| 1.6 Structure | 4 |
| 1.7 Recommendations | 4 |
| 1.8 Effective Date..... | 4 |
| SECTION 2.0: RESPONSIBILITIES..... | 5 |
| 2.1 HQMC C4 CyberSecurity Division | 5 |
| 2.2 Commanding Generals (CG) / Commanding Officers (CO) | 5 |
| 2.3 ISSM and ISSO | 6 |
| 2.4 Privileged Users | 7 |
| SECTION 3.0: POLICY..... | 8 |
| 3.1 Background | 8 |
| 3.2 Defining the Workforce | 8 |
| 3.3 Qualification Requirements | 12 |
| 3.4 Training the Workforce..... | 13 |
| 3.5 Certifications and Waivers | 15 |
| 3.6 Sustainment | 21 |
| SECTION 4.0: REFERENCES | 22 |
| SECTION 5.0: ACRONYMS..... | 24 |

TABLE OF FIGURES

Figure 1. DoD Approved Baseline Certifications..... 10
Figure 2. USMC Approach to a Qualified Cybersecurity Workforce 12
Figure 3. DoD CIO Defined Cyberspace Domain 13
Figure 4. IAT Categories 16
Figure 5. IAM Categories 17
Figure 6. CND Categories..... 18
Figure 7. IASAE Categories 19

This page intentionally left blank

EXECUTIVE SUMMARY

Current Federal cybersecurity and Computer Network Defense (CND) regulations require users of Federal information resources to have the adequate skills, knowledge, and training to manage information resources, thereby enabling the Federal government to effectively serve the public through automated means. Federal law and regulations require agencies to identify, train, track, and report personnel through the most efficient means available. This process, along with supportive references, provide the necessary methodology to properly execute the requirements stated in accordance with United States Marine Corps (USMC), Department of the Navy (DON), Department of Defense (DoD), federal standards, laws, and regulations. The scope of regulated policy and requirements related to Information Assurance responsibilities has intensified to keep up with advancing technologies and now includes Cybersecurity, integrating intelligence and law enforcement activities into current practices.

It is the intent for the Marine Corps to align with the National Initiative for Cybersecurity Education (NICE) Cybersecurity Workforce Framework in addition to amplifying the Information Assurance Workforce (IAWF) into the Cybersecurity Workforce (CSWF). This order augments DoD directives, instructions, and guidance governing cybersecurity to be followed by Marine Corps commands and directorates in applying uniform standards for identifying, training, tracking, and reporting USMC CSWF personnel that operate, maintain, program, manage, or supervise Information Technology (IT) systems and resources.

This page intentionally left blank

SECTION 1.0: INTRODUCTION

1.1 BACKGROUND

MCO 5239.2A, reference (a), formally establishes the MCCSP and defines the responsibilities for protecting the Marine Corps information infrastructure as well as delineating DoD directives, instructions, and guidance governing DoD cybersecurity. In accordance with reference (a), detailed cybersecurity practices and procedures supporting the MCCSP will be published and released by Headquarters Marine Corps (HQMC) Command, Control, Communications, and Computers (C4), Cybersecurity Division (CY) through supplemental cybersecurity guidance, updates, or revisions provided through ECSDs.

The need for trained and knowledgeable Marine Corps CSWF professionals has always been a part of the growth and advancements in technology. The Marine Corps has always taken close interest in providing well-developed training curriculums, from basic training and Military Occupational Specialty (MOS) schools through advanced courses and career specific training, for Marines and Civilian personnel. The field of IT is no exception but is now providing standard baselines for which specific skills can be measured.

The IT field has significantly outpaced growth rates of other industries and keeping up with changes in skills and knowledge can be a challenging task. In 2005, the Defense Information Assurance Program (DIAP), within reference (b), attempted to create standards within the DoD that resulted in the creation of the Information Assurance Workforce Improvement Program (IA WIP) and the requirement to train and employ a qualified workforce based on established standards for the field and assists the industry in supporting these efforts.

1.2 PURPOSE

MCO 5400.52, reference (c), DON Deputy Chief Information Officer Marine Corps Roles and Responsibilities, assigns responsibility for all networks and networked systems within Marine Corps to HQMC C4.

This directive augments DoD directives, instructions, and guidance governing Cybersecurity training and requirements set forth for personnel that fall under the CSWF, to include the delineation of responsibilities for Marine Corps commands and directorates. The intent of the Marine Corps CWIP is to establish standardized training and qualification requirements for the CSWF and ensure the appropriate planning for commands and personnel with the level of knowledge and skills that reinforces the protection of communication and information resources by those using and managing IT systems. Some of the key aspects in references (d) through (j) will be reiterated in this document with additional requirements that will reinforce and enhance the CWIP, specifically for the Marine Corps, and is to be used as a supplemental guide to the program.

1.3 APPLICABILITY AND SCOPE

1.3.1 Applicability

This Directive applies to:

- Marine Corps components, organizations, and personnel (government and non-government employees) that operate aboard Marine Corps facilities or access Marine Corps IT systems. This includes any networks that process any Marine Corps data whether stand alone, contractor provided, or directly connected to the MCEN backbone.
- The MCEN is the Marine Corps network-of-networks and approved interconnected network segments. It comprises people, processes, logical and physical infrastructure, architecture, topology, and Cyberspace Operations that operate according to Marine Corps policy.
- This directive applies to all CSWF personnel that are responsible for creating, programming, maintaining, managing, and supervising DoD Information Systems (IS) and resources, inclusive of military, civilian, contracted, and foreign nationals attached to, serving with, or temporarily assigned to any Marine Corps command.

1.3.2 Scope

The standards identified in this Directive will be used as a resource by all Marine Corps organizations and departments that acquire, develop, use, and maintain information systems to include contracted third-parties who use commercial wireless devices, services, networks, and technologies currently used in both ashore and afloat environments on the MCEN.

This Directive will not alter or supersede the existing authorities and policies of the Director of National Intelligence (DNI) regarding the protection of Sensitive Compartmented Information (SCI) and special access programs for intelligence as directed by Executive Order 12333 and other laws and regulations. The application of the provisions and procedures of this Instruction to SCI or other intelligence information systems (ISs) is encouraged where they may complement or address areas not otherwise specifically addressed.

1.3.3 Objectives

To ensure that the Marine Corps:

- Protects the confidentiality, integrity, availability, authentication, and non-repudiation of Marine Corps ISs, network devices, services, and technologies. These protections include protecting the data at rest and data in transit as well as protecting the network that these devices operate on.
- Provides training to personnel administering and maintaining Marine Corps ISs and network devices commensurate with their duties and responsibilities.
- Ensures related technology research and development efforts are responsive to Marine Corps requirements.
- Encourages interoperability between Marine Corps, DON enclaves, Federal, and DoD agencies, as required.

- Ensures compliance with this Directive as well as other DoD, DON, and Secretary of the Navy (SECNAV) policies, instructions, and directives.

1.3.4 Action

This Directive takes precedence over all previous Marine Corps messages, instructions, and policies concerning certification and accreditation.

- All Marine Corps Commands will implement this Directive within their organizations.
- All operating activities will budget for and execute the actions necessary to comply with this Directive.

1.4 CANCELLATION

This document cancels MarAdmin 689/10, dated 22 Dec 2010, and MarAdmin 722/10, dated 22 December 2010.

1.5 DISTRIBUTION

This Directive is approved for limited distribution to only those individuals possessing DoD Public Key Infrastructure (PKI) certificates and an official need to access this directive. To obtain access to Enterprise Cybersecurity Directives go to the HQMC C4, CY web page at:

https://ehqmc.usmc.mil/org/c4/cy1/doclib/1_cybersecurity_division_public_library/

1.6 STRUCTURE

This Directive is organized into five major sections: (1) Defining the Workforce; (2) Qualification Requirements; (3) Training the Workforce; (4) Certification and Waivers; and, (5) Sustainment.

1.7 RECOMMENDATIONS

Recommendations for change or amendment to this Directive will be submitted in writing through the HQMC C4, CY at:

M_HQMC_C4_CY_ENT_UD@usmc.mil

Recommendations for changes to this directive will be evaluated before taking the necessary action to change or amend this particular ECSD.

1.8 EFFECTIVE DATE

This Enterprise Directive is effective upon signature of the Director, HQMC C4.

SECTION 2.0: RESPONSIBILITIES

2.1 HQMC C4 CYBERSECURITY DIVISION

HQMC C4 CY is responsible for:

2.1.1 Providing guidance and resources, as the lead, on all requirements and execution of the CWIP in accordance with references (a), (e), and (g).

2.1.2 Ensuring initial IA orientation and annual awareness training are available to all authorized users to ensure they know, understand, and can apply the IA requirements of their system(s) in accordance with reference (d) and will eventually be updated with the publishing of the Department of Defense Directive (DoDD) 8140 in May 2014.

2.1.3 Providing representation as the service CWIP Office of Primary Responsibility (OPR) at all DIAP functions and meetings to develop enterprise resources and support CSWF management requirements defined in law, executive orders, and DoD issuances.

2.1.4 Serving as a voting member of the DIAP Certification Committee.

2.1.5 Providing representation on the DON CSWF Management, Oversight, and Compliance Council (MOCC) Executive Board.

2.1.6 Collecting metrics pertaining to reporting requirements submitted to the DoD Chief Information Officer (DoD CIO) and analysis of the CSWF and annual Federal Information Security Management Act (FISMA) in accordance with references (e) and (k) to be captured within Marine Corps Training Information Management System (MCTIMS) per references (l), (m), and (n).

2.1.7 Establishing the appropriate processes, procedures, and policies to ensure service component compliance of the program at the DIAP level.

2.1.8 Integrating and enforcing policy requirements, as mandated in reference (h), with the Inspector General of the Marine Corps (IGMC) for distribution under the Command Inspection Programs (CIP) and Unit Inspection Programs (UIP) in accordance with reference (o).

2.1.9 Updating these standards as required.

2.2 COMMANDING GENERALS (CG) / COMMANDING OFFICERS (CO)

CGs and COs are responsible for:

2.2.1 Establishing local implementation and sustainment plans for CSWF training, commercial certification, management, reporting, and documentation requirements as required in this document and references (d) through (j).

2.2.2 Assigning manpower, personnel, and training responsibilities to local human resources, administrative, and training officers to carry out the CWIP.

2.2.3 Ensuring all CSWF personnel within the command are certified and qualified to include funding of training, certifications, and annual maintenance fees for commercial certifications in coordination with Command Information System Security Manager (ISSM) guidance and recommendations.

2.2.4 Authorizing command ISSMs and Information Systems Security Officers (ISSOs) to ensure compliance through appointments and command directives.

2.3 ISSM AND ISSO

ISSMs and ISSOs are responsible for:

2.3.1 Identifying all positions performing information systems management, specialized, or privileged access cybersecurity functions by category, specialty, and level as described in reference (d). This applies to all positions with cybersecurity duties, whether performed as primary or additional/embedded duties. This requirement applies to military and civilian positions including those staffed by local nationals (LNs).

2.3.2 Identifying all cybersecurity function requirements to be performed by contractors in their statement of work/contract including LNs. Ensure contractors are appropriately certified, and have the appropriate background investigation to perform those cybersecurity functions per reference (e).

2.3.3 Training, certification, and obtaining the proper background investigation for all military and civilian personnel identified as part of the cybersecurity workforce to accomplish their cybersecurity duties per reference (e).

2.3.4 Ensuring cybersecurity personnel performing cybersecurity functions obtain/maintain a commercial certification corresponding to the highest level function(s) required by their position per reference (e).

2.3.5 Obtaining the appropriate background investigation, per reference (e) and (q), prior to granting unsupervised privileged access or management responsibilities to any DoD system.

2.3.6 Identifying, tracking, and monitoring cybersecurity personnel performing IA functions, per reference (e), to ensure that cybersecurity positions are staffed with trained and commercially certified personnel.

2.3.7 Ensuring that all CSWF personnel within their command understand and comply with requirements directed in references (a) through (j) by establishing awareness of individual commercial certification requirements of the position assigned and developing individual training and certification compliance requirements;

2.3.8 Tracking all CSWF personnel, training, and certifications within the command and reporting compliance.

2.3.9 Submitting requests, in writing, to HQMC C4 CY, for all CSWF personnel requiring certification waivers via the chain of command in accordance with references (e) and (x).

2.3.10 Coordinating with supervisors and supporting HR organizations to ensure standard language appears in position descriptions which identify the position as being part of the Marine Corps CSWF.

2.4 PRIVILEGED USERS

Privileged Users, as authorized by ISSMs, are responsible for:

- 2.4.1** Understanding and complying with command cybersecurity policies and procedures.
- 2.4.2** Completing user form (DD Form 2875) and privileged access agreements as required by reference (g).
- 2.4.3** Completing appropriate security background checks in accordance with reference (p) and (t).
- 2.4.4** Reporting qualification status to the appropriate ISSM and the highest-level certification achieved in the Defense Workforce Certification Application (DWCA) (<https://www.dmdc.osd.mil/appj/dwc/index.jsp>); and MCTIMS (<https://mctims.usmc.mil>) for Marine Corps FISMA tracking and to assist with Annual Maintenance Fee (AMF) payment processing that will be managed at the local command through fiscal or purchasing agent in accordance with reference (m).

SECTION 3.0: POLICY

3.1 BACKGROUND

The implementation of the CWIP has left many challenges to adapt to the dynamic field of cybersecurity. Responsibilities for many positions overlap other functional areas in the field and quickly fall outside the parameters of traditional job titles.

Personnel assigned to cybersecurity positions (as required by references (e), (h), (i), and (s)), or Certification and Accreditation (C&A) roles (as indicated under table T1 of reference (w)), are required to be appointed in writing by the appropriate authority.

3.2 DEFINING THE WORKFORCE

3.2.1 Personnel

The CSWF is defined by Active Duty (AD) Marines, Reserve Marines, Civilian Marines, contractors, and Foreign Nationals. These personnel may fall within the defined IA Technical (IAT), IA Management (IAM), Computer Network Defense (CND), or IA Security Architect and Engineer (IASAE) job categories per reference (e).

3.2.1.1 Military

Marine Corps Active Duty and Marine Corps Reserve enlisted and officers performing cybersecurity functions as listed above in section 3.2.1.

3.2.1.2 Civilian Marines

Civilian Marines within the CSWF are captured in the Cyber / IT Workforce Community located on the DON Civilian Human Resources website located at:

(<http://www.public.navy.mil/donhr/TrainingDevelopment/ccmgmt/Pages/CivilianCommunities.aspx>.) When possible, CSWF billets shall be classified by General Schedule (GS) parenthetical specialty title. Enter the appropriate parenthetical specialty title for the primary function in the Defense Civilian Personnel Data System (DCPDS) or equivalent civilian personnel database. This is required for all DoD personnel, even if the individual performs more than two specialties. Civilian Marines in the CSWF job series' will need to update their position descriptions by their supervisors with the follow statement:

"Employee shall obtain and maintain the proper cybersecurity certification for the cybersecurity position as required in the DoD 8570.1-M. Upon request of the ISSM, the employee shall provide documentation supporting the cybersecurity certification status. The employee and his or her supervisor shall ensure the employee maintains certification status. Certification and maintenance requirement for the certification shall be at no cost to the employee. Certified CSWF personnel performing cybersecurity functions whose certification lapses shall have their access to DoD information systems either downgraded to a level appropriate for their certification status or denied access to DoD information systems. Personnel must allow commercial certification providers to report their certification status to the DON."

3.2.1.3 Contractors

Contracted cybersecurity functional requirements must be identified in their statement of work/contract and in compliance with DoD 8570.01-M for the category and level functions they are performing. See Defense Acquisition Regulations System, 48 CFR Parts 239 and 252, RIN 0750-AF52, Defense Federal Acquisition Regulation Supplement; Information Assurance Contractor Training and Certification (DFARS Case 2006-D023) for further clarification. Ensure contractors are appropriately certified and have the appropriate background investigation to perform those cybersecurity functions per reference (a). Funding for contractor training, certifications, and maintenance fees will not be paid for by the Marine Corps.

3.2.1.4 Foreign Nationals (FNs)

FNs are non-U.S. citizens or immigrant aliens whom are employed by DoD organizations and may be considered civilian or contracted personnel. Military service members who are FN's and fall under the Uniform Code of Military Justice (UCMJ) are to be considered military personnel for the purpose entitlements and benefits under the CWIP. FN's are restricted to the assignment of certain cybersecurity positions and security clearances under references (p) and (w) respectively. FN's are entitled to the training and benefits provided under their employment status, whether direct hire as civilian personnel or non-direct hire as contractor personnel. This is only if the parameters and the clearance level can be attained in accordance with references (p) and (w).

3.2.2 Function

3.2.2.1 Privileged Access

The CSWF consists of a significant number of personnel that support Marine Corps communication and information assets. All personnel who have privileged access to systems are to be considered part of the CSWF and are Enabled Privileged Users (EPUs) that:

- a. Have supervised privileged access
- b. Are currently training through formal, military, or on-the-job training
- c. Are not in a billet or position that requires CSWF qualification criteria to be met
- d. Have unsupervised privileged access
- e. Are in a billet or position that requires CSWF qualification criteria to be met
- f. Have been placed in a billet of higher qualification criteria and meets at least one category/level qualification requirement at a lower level.

Personnel that need privileged access to information resources are required to complete the Privileged Access Agreement Form (DD Form 2875 SAAR), which satisfies the requirements for the policy under reference (e). Prior to granting privileged access, personnel must meet the minimum security clearance and investigation requirements under reference (p). Privileged access is explicitly authorized access authority, as defined in reference (z), or authorized capabilities to perform security-relevant functions that ordinary users are not authorized to perform with authentication, authorization or accounting abilities into any government information resource and may also be referred to as administrative or root access. It is also defined in reference (g) and includes law enforcement personnel and inspectors conducting investigations into legal or compliance related functions.

3.2.2.2 Positions/Roles

Personnel assigned to IT related administrative functions, to include policy makers, Acquisitions, Technology & Logistics (AT&L), intelligence communities, law enforcement activities, and C4 functions related to cybersecurity shall be identified and comply with policies related to this directive as directed by their supervisor or supporting ISSM. These are not just GS-2210, IT Specialist functions and could meet the criteria in any of the following list and captured by supporting ISSM:

<http://www.public.navy.mil/donhr/TrainingDevelopment/ccmgmt/Pages/CivilianCommunities.aspx>.

Positions/billets that need to be evaluated as part of the CSWF should meet at least one of the criteria listed in the determination matrix per the DoD approved baseline certification list located at http://iase.disa.mil/eta/iawip/content_pages/iabase.html with a recent version of the chart as of March 23, 2014 provided below.

Table AP3.T2 DoD Approved Baseline Certifications

| IAT Level I | | IAT Level II | | IAT Level III | |
|--|---|---|---------------------|---------------------|--|
| A+-CE Network+ CE SSCP CCNA-Security | GSEC Security+ CE SSCP CCNA-Security | CISA CSE GCIH GCED CISSP (or Associate) CASP | | | |
| IAM Level I | | IAM Level II | | IAM Level III | |
| CAP GISP GSLC Security+ CE | CAP GSLC CISM CASP CISSP (or Associate) | GSLC CISM CISSP (or Associate) | | | |
| IASAE I | | IASAE II | | IASAE III | |
| CISSP (or Associate) CASP CSSLP | CISSP (or Associate) CASP CSSLP | CISSP - ISSEP CISSP - ISSAP | | | |
| CNDSP Infrastructure Support | | | | | |
| CNDSP Analyst | | CNDSP Incident Responder | | CNDSP Auditor | |
| GCIA CEH GCIH | SSCP CEH | GCIH CSIH CEH GCFA | CISA GSNA CEH | CISSP-ISSMP CISM | |

Figure 1. DoD Approved Baseline Certifications

3.2.3 Reporting

3.2.3.1 Marine Corps Authoritative Database

Command ISSMs are required to track their CSWF within their command and report all personnel in MCTIMS, which is the authoritative database management system used to track the CSWF.

3.2.3.2 Defense Workforce Certification Application (DWCA)

All personnel holding a certification within a defined IAT, IAM, CND, or IASAE job category must release their certification information to the DoD through DWCA:

(<https://www.dmdc.osd.mil/appj/dwc/index.jsp>).

3.2.4 NICE Cybersecurity Framework

The ability of academia and public and private employers to prepare, educate, recruit, train, develop, and retain a highly-qualified CSWF is vital to our nation's security and prosperity. In recognition of the criticality of these issues, President George W. Bush established the Comprehensive National Cybersecurity Initiative (CNCI). The workforce aspect of the CNCI was specifically emphasized and reinforced in 2010 when the President of the United States (POTUS) established the NICE, which was formerly CNCI Initiative 8. The NICE is a nationally coordinated effort focused on cybersecurity awareness, education, training, and professional development. Its goals are to encourage and help increase cybersecurity awareness and competence across the nation and to build an agile, highly skilled cybersecurity workforce capable of responding to a dynamic and rapidly evolving array of threats. Free Cybersecurity training can be located on the NICE website at <http://niccs.us-cert.gov/training/tc/search> located on the National Initiative for Cybersecurity Careers and Studies (NICCS) website.

NICE has developed the National Cybersecurity Workforce Framework ("the Framework") to provide a common understanding of and lexicon for cybersecurity work. Defining the cybersecurity population consistently, using standardized terms is an essential step in ensuring that our country is able to educate, recruit, train, develop, and retain a highly-qualified workforce. As the DoD slowly migrates and adapts this framework, further clarification and guidance will be distributed by HQMC C4 through official correspondence updates.

In designing the Framework, "Categories" and "Specialty Areas" were used as an organizing construct to group similar types of work. The categories, serving as an overarching structure for the Framework, group related specialty areas together. Within each specialty area, typical tasks and knowledge, skills, and abilities (KSAs) are provided. In essence, specialty areas in a given category are typically more similar to one another than to specialty areas in other categories.

This framework organizes cybersecurity into seven high-level categories, each comprised of several specialty areas, that will be utilized to help define the USMC CSWF as it is integrated with the DoD and DON and will include:

- a. Securely Provision – specialty areas concerned with conceptualizing, designing, and building secure IT systems, with responsibility for some aspect of the systems' development
- b. Operate and Maintain – specialty areas responsible for providing the support, administration, and maintenance necessary to ensure effective and efficient IT system performance and security

- c. Protect and Defend – specialty areas responsible for the identification, analysis, and mitigation of threats to internal IT systems or networks
- d. Investigate – specialty areas responsible for the investigation of cyber events and/or crimes of IT systems, networks, and digital evidence
- e. Operate and Collect – specialty areas responsible for the highly specialized collection of cybersecurity information that may be issued to develop intelligence
- f. Analyze – specialty areas responsible for highly specialized review and evaluation of incoming cybersecurity information to determine its usefulness and intelligence
- g. Support – specialty areas providing support so that others may effectively conduct their cybersecurity work

3.3 QUALIFICATION REQUIREMENTS

Below, Figure 2 depicts the five steps required to be qualified in the CSWF.

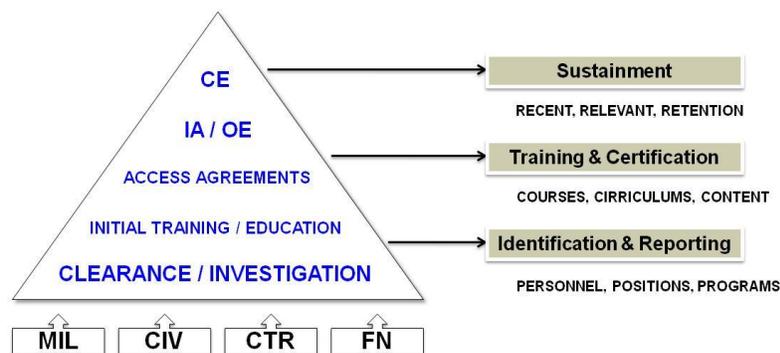


Figure 2. USMC Approach to a Qualified Cybersecurity Workforce

3.3.1 Background Investigation and Clearance

A cleared background investigation is required for each individual in the CSWF in accordance with reference (p).

3.3.2 Standardized Training

Military personnel are provided standardized training through MOS schools and completion of any IT/IS related curriculum that mandates final examination through proctored testing satisfies the requirement for initial training.

Standardized education requirements may be satisfied for civilians and contractors with an associate degree, undergraduate degree from an accredited university, or a graduate/postgraduate degree in an IT/IS related field.

3.3.3 Access Agreements

A series of forms have been provided to document access to DoD IS for user and enhanced services based on references (e), (g), (h), (u), (v), and (y). Each user with access to DoD IS shall comply with policies that are used to govern and protect information assets. This may include system, privileged, remote, and Portable Electronic Device (PED) and Secured Mobile Environment Portable Electronic Device (SME-PED) access agreements used to identify provisions in the regulations and use of capabilities, responsibilities, and requirements.

3.3.4 Baseline IA Certification

Baseline IA certifications establish minimum standards for knowledge related to cybersecurity.

3.3.5 Operating Systems Environment

Operating Systems Environment establishes the minimal technical knowledge required for a system. The 8570.01-M divides Operating System (OS) environments into Computing Environment (OS/CE), Network Environment (OS/NE), and Enclave Environments (OS/EE).

3.4 TRAINING THE WORKFORCE

Training shall be the responsibility of the owning command per references (n) and (aa). CSWF should utilize e-learning strategies through such options as the NICCS website as well as the training information to follow, since this training is "no cost" to the individual command. Any training that is beyond the requirement of the position being fulfilled will be at the cost of the individual, unless the job description is changed to reflect current duties and responsibilities. Members of the CSWF can be aligned to any of the below areas of responsibility as defined by the DoD CIO in their mapping of the DoD Cyberspace Domain as depicted in Figure 3.

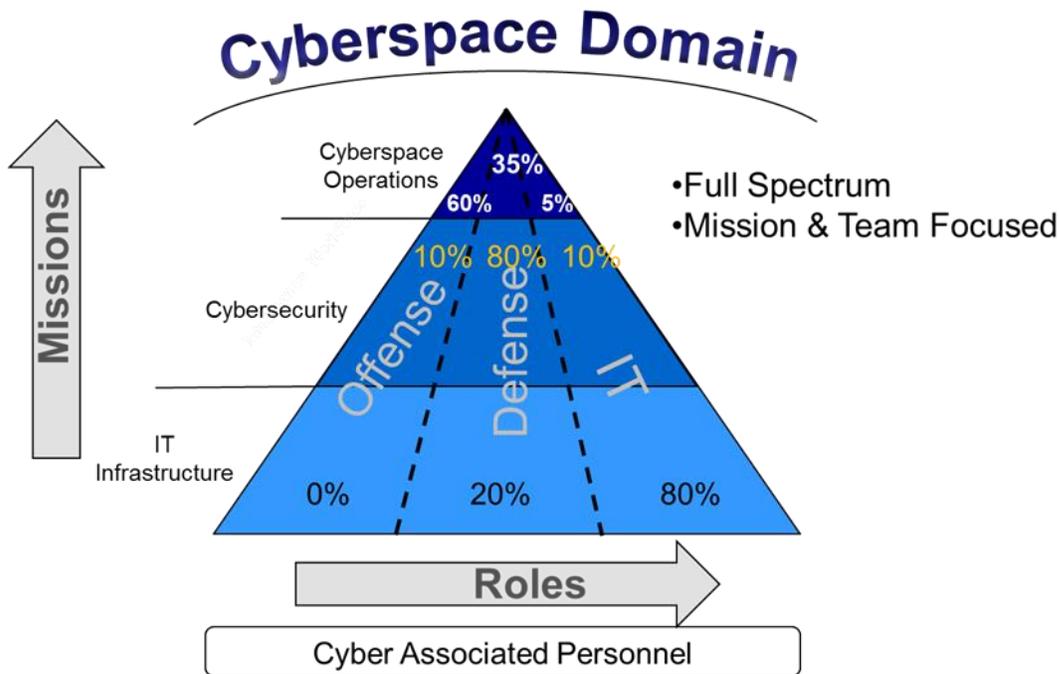


Figure 3. DoD CIO Defined Cyberspace Domain

3.4.1 Marine Corps Communication Electronic School (MCCES)

MCCES will continue to conduct 8570 training under the Cyber Network Specialist Course, Cyber Network Supervisor Course, Information Assurance Technician Course, Cyber System Chief Course, Communications Chief Course, Microsoft Academy, CISCO Academy, and any future training curriculum that is certified to be taught.

3.4.2 Communication Training Centers (CTCs)

Training is currently available through CTCs located at each of the Marine Expeditionary Forces (MEFs). Additional information is provided below and is MEF dependent, so coordination with local CTC and MEF is required for further clarification. General guidelines are provided and at the discretion of the local CTC per reference (m).

In order to receive a voucher for a certification exam through the CTC, Marines and Civilian Marines must be designated by their Major Subordinate Command (MSC) ISSM as a current member of the CSWF in MCTIMS. MCTIMS will be used as the authoritative database to determine eligibility. Enrollments need to be submitted at least two weeks prior to the course start date to ensure vouchers will be available for testing at the completion of a certification course. Vouchers may not be available for Marines or Civilian Marines who have their enrollments submitted after the two-week window. Each CTC will ensure the students pass a pretest before issuing a voucher for the certification exam.

Marines and Civilian Marines will only receive a testing voucher for the certification exam that aligns with their IA level in MCTIMS. Coordination with CTC and MSC ISSM is critical to ensure users will have the ability to possibly attend the following courses and/or take these exams.

- a. IAT Level 1 - IA: A+ or Network+; OS/CE: MCP or CCENT
- b. IAT Level 2 - IA: Security+; OS/CE: MCITP or CCNA
- c. IAT Level 3 - IA: CISSP; OS/CE: MCSE or CCNP
- d. IAM Level 1 - IA: Security+
- e. IAM Level 2 - IA: GSLC, CISM, CISSP
- f. IAM Level 3 - IA: GSLC, CISM, CISSP

Marines and Civilian Marines who are appropriately certified according to their IA level will not be given vouchers for additional certifications. For example, if you are an IAT Level 2 and have Security+, you will not be given a Network+ voucher.

Marines and Civilian Marines in the CSWF will take priority in all classes while others will be considered on a stand-by basis only (to include other Services). Marines and Civilian Marine who are not in the CSWF are eligible to attend the training, as long as they meet the associated pre-requisites, with the understanding that they will not be given a testing voucher. Those Marines who desire to take the certification exam will have to pay for their own voucher. Further information on POCs is as follows:

- a. MCCES Warfighting Support Branch SNCOIC – (760) 830-1269
- b. CTC-1 (I MEF) - (760) 763-7029
- c. CTC-2 (II MEF) - (910) 451-2878
- d. CTC-3 (III MEF) - (315) 623-1053

3.4.3 MarineNet

MarineNet is another web based training option available at the following website: (<https://www.marinenet.usmc.mil/MarineNet/GetCACUser.aspx>). The Marine Corps Information Technology Community of Interest is building specific curriculum to provide to the cybersecurity workforce and include on MarineNet. Civilian Marines, FN, and contractors requiring access to MarineNet should request an account in accordance with reference (cc).

3.4.4 Federal Virtual Training Environment (FedVTE)

Web based courses are available through Federal Virtualized Training Environment (FedVTE), which is hosted and managed by Department of Homeland Security (DHS). Accounts can be requested on the FedVTE at the following website: (<https://www.fedvte-fsi.gov/Vte.Lms.Web>) or by emailing HQMC C4CY FedVTE administrators at IAWF@USMC.MIL. All Members of the USMC CSWF community are eligible for access to FedVTE training material at no cost under a sponsorship program funded by the DoD and Department of State. Eligibility requires that you provide your .mil email address and approval from the MSC ISSM when requesting access in accordance with reference (bb).

3.4.5 Marine Corps Cybersecurity Consortium

As approved, HQMC hosts the Marine Corps Cybersecurity Consortium (MCCYC), which provides multiple training courses from the approved 8570 baseline certifications list as well as current and cutting edge training.

3.4.6 Commercial Vendors

Commands may utilize commercial vendors to provide training in support of this directive. Although more costly, it offers the flexibility to meet training requirements based on operational tempo.

3.4.7 TWMS

The Total Workforce Management System (TWMS) (<https://twms.nmci.navy.mil/login.asp>) is a web-based tool designed to support efforts in managing the workforce from various perspectives throughout a command or enterprise. A TWMS user account is no longer necessary to view the information of employees assigned directly under your supervision. In your own Self Service record (<https://twms.nmci.navy.mil/selfservice>) there is a new button on the left called 'MY WORKFORCE'. When you click on it, the records of all personnel directly assigned to you, and their billet data, becomes available exactly as if you had a TWMS Manager account. For those who need access to the second-line subordinate employees, the TWMS Manager Account will still be an option. For more information please download the MY WORKFORCE FAQ below. Marine Corps users are able to seek further information by accessing: https://www.manpower.usmc.mil/portal/page/portal/M_RA_HOME/MP/MPC/d_CWM/TWMS.

3.5 CERTIFICATIONS AND WAIVERS

3.5.1 Certification Categories

All levels within the IAT, IAM, CND, and IASAE categories are required to meet qualification requirements for certifications in IA and training in their primary Operating System Environment. Training normally culminates in vendor-specific training and completion certificates; however, there may be instances of factory training or Systems Command training that may result in a certificate. The actual certification tests can be taken at Marine Corps CTCs, or at a vendor approved testing center (e.g., Pearson Vue, Prometric). In cases where service mandated training is judged to meet a baseline standard, the command ISSMs can request exception to the commercial training requirement to HQMC. HQMC C4 CY will review and may approve the training standard. Additional details are provided in paragraph 3.5.5 of this directive.

3.5.2 IAT Category

The IAT is responsible for any technical category cybersecurity functions and must be certified to the highest level of functions performed in accordance with reference (e). IAT personnel make the systems less vulnerable by implementing technical controls on the Information Systems (IS). These systems and their corresponding IAT level range from local user support (LAN) to Wide Area Network (WAN) technical support. These duties may align with specific technical roles:

- a. Systems Administrator
- b. Desktop Administrator
- c. Help Desk Technician
- d. Information Systems Technician
- e. Network Administrator
- f. Intrusion Detection and Prevention
- g. Auditing

Figure 4 provides IAT categories and is available in the following link:

https://www.cool.navy.mil/ia_documents/ia_iaat_flow.htm

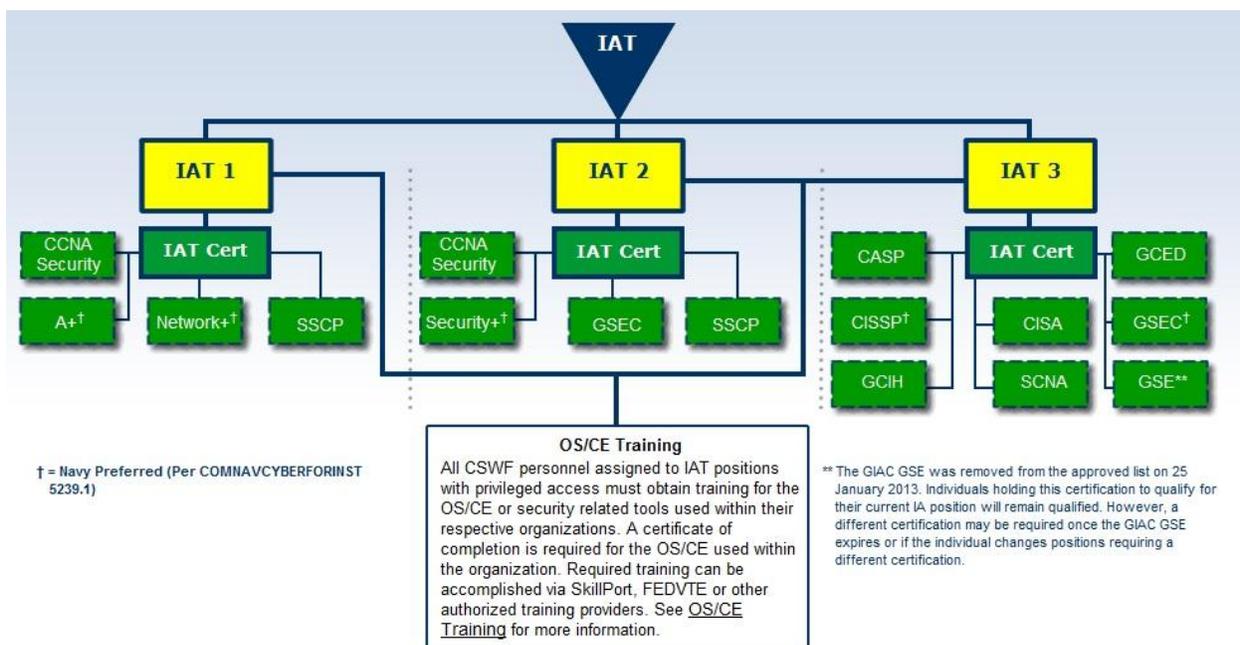


Figure 4. IAT Categories

3.5.3 IAM Category

In accordance with Department of Defense Instruction (DoDI) 8570 the IAM/Information Systems Security Manager (ISSM) is responsible for ensuring the information system (IS) is implemented, operated, used, maintained, and disposed of in accordance with security policies and practices per references (e) and (g). CSWF personnel that fall under the IAM category shall train, certify, and sustain their cybersecurity baseline certification as a part of their qualification requirements in accordance with reference (d). Any personnel in the IAM/ISSM role performing IAT duties will also have the appropriate IAT level certification per reference (e). The duties as an IAM/ISSM, per reference (a), may align with the following functional roles:

- a. Information Assurance Officer (IAO)/ Information Systems Security Officer (ISSO)
- b. Information Assurance Manager (IAM)/ Information Systems Security Manager (ISSM)

Figure 5 provides the IAM Categories and is available in the following link:

https://www.cool.navy.mil/ia_documents/ia_iam_flow.htm.

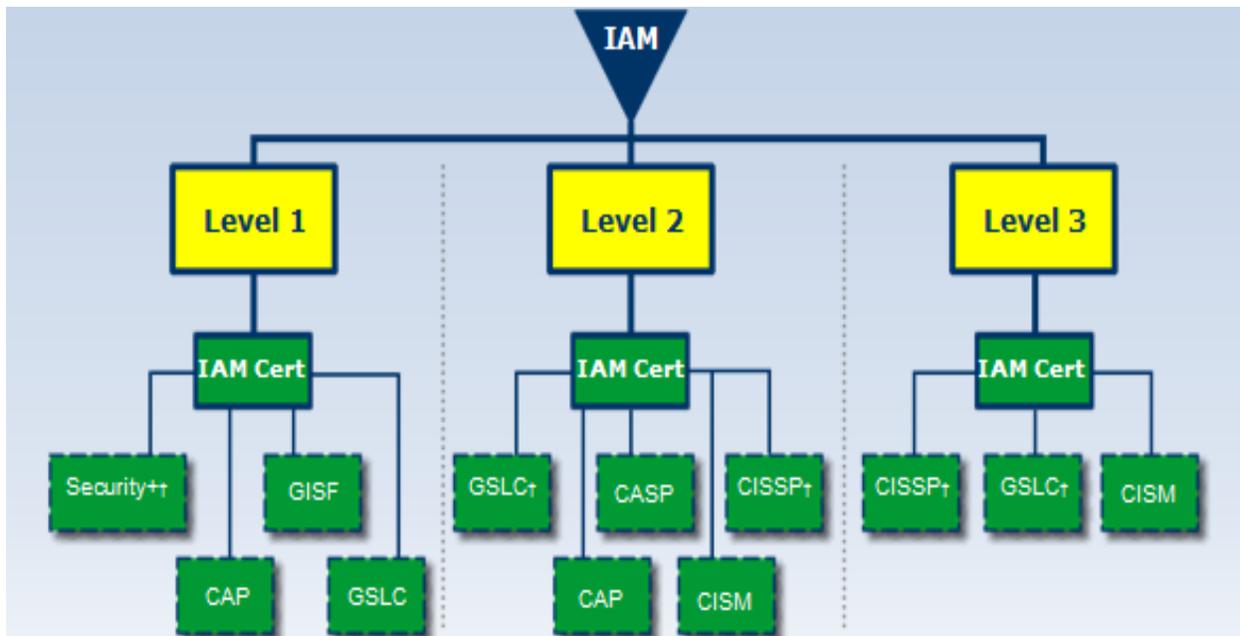


Figure 5. IAM Categories

3.5.4. Computer Network Defense – Service Provider (CND-SP) Categories

The primary CND service areas are to: protect; monitor; analyze and detect; and respond. These services include actions used for preventing or mitigating computer network attacks that may cause disruption, denial, degradation, destruction, exploitation, or access to computer networks, information systems, or the theft of information. The duties as a CND-SP align with the following roles:

- a. CND-SP Analyst (CND-A)
- b. CND-SP Infrastructure Support (CND-IS)
- c. CND-SP Incident Responder (CND-IR)
- d. CND-SP Auditor (CND-AU)
- e. CND-SP Manager (CND-SPM)

These items are further broken out into functional areas as provided in the graph below and in accordance with the DON CIO CND Roadmap.

Figure 6 provides the CND categories and is available in the below link:

https://www.cool.navy.mil/ia_documents/ia_CND_flow.htm.

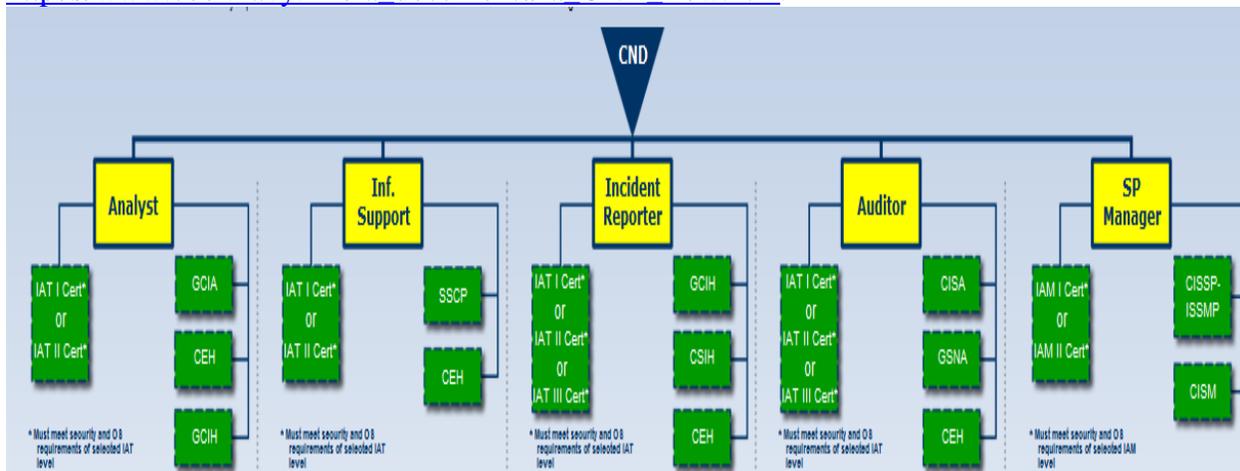


Figure 6. CND Categories

3.5.5. IASAE Categories

Information Assurance System Architect and Engineer (IASAE) functions are focused primarily at the Echelon II and MSC level to support system acquisition and development, to include design, development, implementation, and integration of cybersecurity systems per reference (e). Some job functions may occur in Echelon III commands when acting as the Research, Development Test & Evaluation (RDT&E) IA Architecture or Lead Security Engineer representative for the Echelon-II AQ/Development office. Contractors may perform IASAE functions appropriate to their certification level, but may not be able to perform all IASAE functions. IASAE functions relating to requirements generation and entry of requirements into Statements of Work will normally require government personnel or direct government supervision per reference (g). The duties as an IASAE may align with the following roles:

- a. Systems Engineer
- b. Network Engineer
- c. Computer Scientist
- d. Computer Specialist

Figure 7 provides IASAE categories and is available in the following link:
https://www.cool.navy.mil/ia_documents/ia_iasae_flow.htm

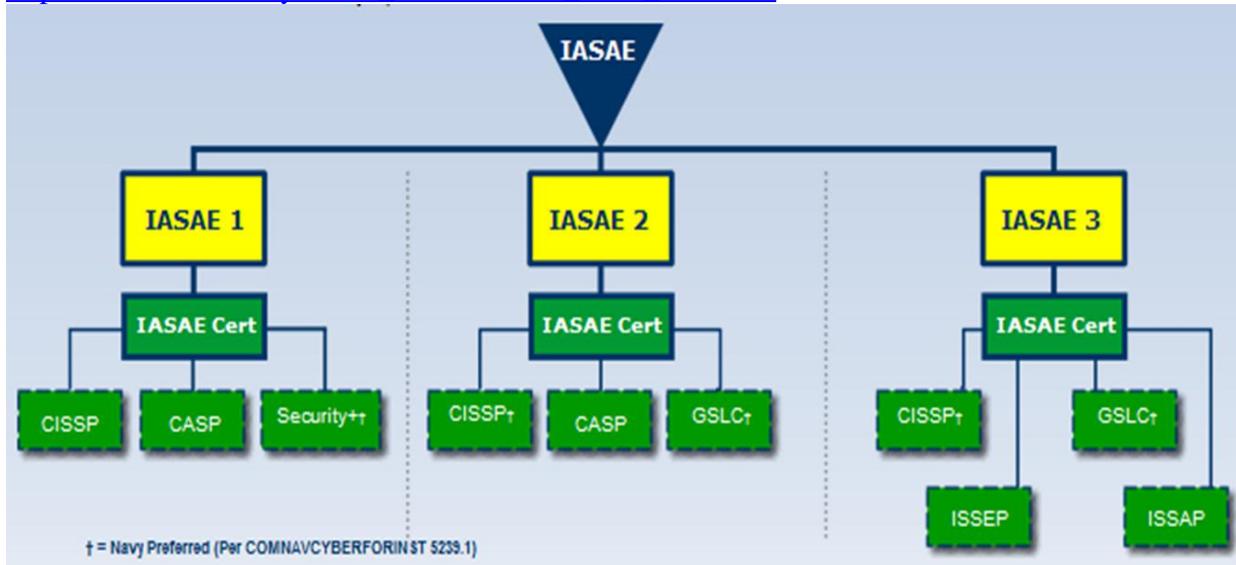


Figure 7. IASAE Categories

3.5.6. Certification Vouchers

Individuals must pass a pre-test prior to receiving a voucher. Pre-tests can be completed using one of three different methods. The first method is by testing at the Marine Corps Communications and Electronic School (MCCES), after attending a course hosted by the CTC. The second method is to request a pre-test from one of the CTCs via email/telecom as directed in reference (m). The third method is to take the pre-test on-line through the CTC.

- a. One certification voucher can be issued at your local CTC in order to complete the baseline certification exam for the billet and job category held.
- b. If the individual does not pass the exam they will not be issued another voucher from the CTC.
- c. Secondary vouchers for the failed exam may be provided by the command; however, it is at the discretion of the command to determine funding availability for secondary vouchers.
- d. If the individual does not pass the exam the second time it will be the responsibility of the command to determine the next course of action (i.e., retest, reassignment, or termination from that billet).
- e. Vouchers for individuals who have already met the baseline certification requirements may be provided by the local command; however, it is at the discretion of the command to determine funding availability for secondary certifications.

3.5.7. Cybersecurity Baseline Certifications

Cybersecurity certifications are based on the DoD IA approved baseline certification chart located in reference (e). Personnel performing cybersecurity functions are authorized to choose any of the approved certifications within their job category to meet the applicable certification requirement for each associated level located at http://iase.disa.mil/eta/iawip/content_pages/iabaseline.html. Additionally, the following guidance applies to all personnel:

- All personnel, as a condition of privileged access to any DoD information systems, shall be adequately trained and certified in order to perform the tasks associated with cybersecurity responsibilities. Personnel performing cybersecurity functions are our first line of defense to detect, prevent, isolate, and contain threats against our network and it is critical to ensure that all positions are filled with qualified personnel.
- Personnel in technical category positions must be issued and retain an appointing letter to their cybersecurity duties including a statement of responsibilities for the system per ref (a). Command ISSM's will maintain a completed copy in the individual's personnel record or with the contracting officer's technical representative for contractors.
- Personnel in management category positions will retain an appointing letter assigning those IA responsibilities for their system per references (a), (r), and (y). If a management category position requires cybersecurity privileged access, a statement of responsibility for the system(s) will also be executed per reference (r).

3.5.8. Operating System / Computing Environment (OS/CE)

Considerations to training and education need to reinforce applied skills and knowledge based on tasking associated to the position. Although certifications are a method used to measure retained knowledge it does not always reflect applied skills. It is not required for the CSWF to attain vendor certifications for their operating environment; however, it is encouraged for the command to support doing so if the training is applicable to duties to the job functions. In accordance with the revised OS/CE certification guidance published in reference (x), a certificate of completion from an authorized training course is acceptable to satisfy the qualification requirements for this category. The ISSM must determine the requisite skills needed to satisfy this requirement with a completion certificate documented in their personnel's Electronic Training Jacket (ETJ) for military personnel and with the minimum standards enforced in reference (y) and civilian and contractor records captured and maintained in TWMS in accordance with reference (cc).

3.5.9. Qualification Waivers

- a. Reference (g) defines the CSWF certification waiver eligibility and requirements as well as the process in which waivers are issued per reference (d). Those personnel eligible for CSWF certification waivers must meet the following criteria:
 - Military personnel may be granted a two year waiver based on their pay entry base date.
 - Warrant Officers and lateral movers may be granted a one year waiver based on their latest MOS school graduation date or MOS assignment date.

- Civilians within six months of hire date.
- Those personnel within six months of assignment of a higher IAT or IAM level billet and meets certification requirements at a lower level to exclude IAT Level I positions.
- During deployment and within six months upon return from a combat environment only if a lower level certification is attained and excludes IAT Level I positions.
- Contractors are not eligible for CSWF certification waivers in accordance with the requirements set forth under paragraph C1.4.4.5 and C2.3.9 in reference (a).
- Have not been previously granted a CSWF certification waiver for the requested category/level.

The Commander, Chief Information Officer (CIO), and MSC ISSM must ensure that each CSWF personnel meet the qualification requirements in addition to being trained and certified in the appropriate IAT, IAM, CND, or IASAE category/level and ensure this information is captured and maintained in within MCTIMS in accordance with references (l), (m), and (n).

3.6 SUSTAINMENT

- a. All CSWF personnel are required to maintain cybersecurity baseline certifications based on established requirements that have been coordinated with the vendors. HQMC will no longer fund sustainment costs for the entire USMC CSWF and delegate this responsibility to local commands. Local commands shall plan for sustainment funding to ensure appropriate support in the local MSC level per references (l), (m), and (aa).
- b. Only one highest achieved cybersecurity baseline certification AMF payment shall be made by the local command, but not both for the same certification or for more than one certification. Any additional requirements imposed on by commands are to be supported, in writing, and have the appropriate funds allocated to sustain the program. Military personnel that are required to maintain certification status while assigned to duties that do not fall under the CSWF may contact HQMC C4 for support, but may require funding at the local command or user level.
- c. CSWF personnel whose position requires a certification and who do not meet annual certification maintenance requirements or have allowed their certification to expire are to be considered unqualified for their position.
- d. HQMC C4 CY has coordinated with vendors for some of the required annual Continuing Education (CE) credits for military schools/exercises to account for annual totals to meet the requirements of reference (j). An update with greater clarification will be provided within a separate correspondence.

SECTION 4.0: REFERENCES

- a) MCO 5239.2A, Marine Corps Cyber Security Program, 18 Jul 2012
- b) Title 10, United States Code, Defense Information Assurance Program
- c) MCO 5400.52, Department of the Navy Deputy Chief Information Officer Marine Corps Roles and Responsibilities, 5 Jan 2010
- d) DoD Directive 8570.01, Information Assurance Training, Certification, and Workforce Management, 23 April 2007
- e) DoD 8570.01-M, Information Assurance Workforce Improvement Program, 24 January 2012
- f) SecNav Instruction 5239.3B, Department of the Navy Information Assurance Policy, 17 June 2009
- g) SecNav Manual 5239.2, DON Information Assurance Workforce Management Manual, 29 May 2009
- h) SecNav Instruction 5239.20, Department of the Navy Cybersecurity/Information Assurance Workforce Management, Oversight, and Compliance, 17 June 2010
- i) COMNAVCYBERFOR Instruction 5239.1, Information Assurance Workforce Improvement Program, 7 January 2011
- j) SecNav Instruction 1543.2, Cyberspace/Information Technology Workforce Continuous Learning, 30 November 2012
- k) Title 44, United States Code
- l) CMC GENADMIN 1212-06, Mandatory Enrollment in the Continuing Education (CE) Program For Cybersecurity Workforce (CSWF) Personnel Holding CompTIA Certifications, 12 December 2012
- m) CMC GENADMIN 1212-07, Funding Guidance for CSWF Certification AMF and Funding of Initial and Re-Take of CSWF Certification Exams, 12 December 2012
- n) CMC White Letter 2-11, Cyber Awareness and Accountability, 23 August 2011
- o) MCO 5040.6H, Marine Corps Readiness Inspections and Assessments, 18 March 2007
- p) DoD 5200.2-R, Personnel Security Program, 16 December 1986
- q) DoD Directive 5200.28, Security Requirements for Automated Information Systems (AISs), 21 March 1988
- r) OMB Circular A-130, Management of Federal Information Resources, Transmittal 4, 30 November 2000
- s) DoD Directive O-8530.1, Computer Network Defense, 8 January 2001
- t) DoD 5200.1-R, Information Security Program, January 1997
- u) DoDI 8500.01 Cybersecurity, 14 March 14
- v) DoD Instruction 8500.2, Information Assurance (IA) Implementation, 6 February 2003

- w) DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP), 28 November 2007
- x) DoDI 8510.01, Risk Management Framework (RMF) for DoD Information Technology (IT), 12 March 14
- y) NavAdmin 107/12, Navy Information Assurance Workforce and Operating System/ Computing Environment Certifications, 29 March 2012
- z) CJCSI 6510.01F, Information Assurance and Support to Computer Network Defense, 9 February 2011
- aa) CNSS Instruction No. 4009, National Information Assurance Glossary, 26 April 2010
- bb) CMC White Letter 1-11, Information Protection, 22 April 2011
- cc) CMC GENADMIN 1302-06, HQMC C4 CSWF Guidance for FedVTE Account Creation and Community Management, 13 February 2013
- dd) MARADMIN 288/13, Updates To Annual Cyber Awareness Training For 2013, 11 June 2013

SECTION 5.0: ACRONYMS

| | |
|---------|---|
| AMF | Annual Maintenance Fee |
| AT&L | Acquisitions, Technology, and Logistics |
| | |
| BIC | Billet Identification Code |
| | |
| C4 | Command, Control, Communication, and Computers |
| C&A | Certification and Accreditation |
| CE | Continuing Education |
| CEU | Continuing Education Unit |
| CG | Commanding General |
| CIO | Chief Information Officer or Command Information Officer |
| CIP | Command Inspection Program |
| CNCI | Comprehensive National Cybersecurity Initiative |
| CND | Computer Network Defense |
| CND-A | Computer Network Defense Analyst |
| CND-AU | Computer Network Defense Auditor |
| CND-IR | Computer Network Defense Infrastructure Responder |
| CND-IS | Computer Network Defense Incident Support |
| CND-SPM | Computer Network Defense Service Provider Manager |
| CO | Commanding Officer |
| CSWF | Cybersecurity Workforce |
| CTC | Communication Training Center |
| CWIP | Cyber Workforce Improvement Program |
| CY | Cybersecurity Division |
| | |
| DCPDS | Defense Civilian Personnel Data System |
| DFARS | Defense Acquisition Regulation System |
| DHS | Department of Homeland Security |
| DIACAP | DoD Information Assurance Certification and Accreditation Process |
| DIAP | Defense Information Assurance Program |
| DNI | Director of National Intelligence |
| DoD | Department of Defense |
| DoDD | Department of Defense Directive |
| DoDI | Department of Defense Instruction |
| DON | Department of the Navy |
| DWCA | Defense Workforce Certification Application |
| | |
| ECSD | Enterprise Cybersecurity Directive |
| EPU | Enabled Privileged Users |
| ETJ | Electronic Training Jacket |
| | |
| FedVTE | Federal Virtual Training Environment |
| FISMA | Federal Information Security Management Act |
| FN | Foreign National |

| | |
|--------|---|
| | |
| GS | General Schedule |
| | |
| HQMC | Headquarters Marine Corps |
| | |
| IA | Information Assurance |
| IAM | Information Assurance Management (8570 category) |
| IAM | Information Assurance Manager (8510 position) |
| IAO | Information Assurance Officer |
| IASAE | Information Assurance Security Architect and Engineer |
| IAT | Information Assurance Technical |
| IAWF | Information Assurance Workforce |
| IGMC | Inspector General of the Marine Corps |
| IS | Information System |
| ISSM | Information Systems Security Manager |
| ISSO | Information Systems Security Officer |
| IT | Information Technology |
| | |
| KSA | Knowledge, Skills and Abilities |
| | |
| LAN | Local Area Network |
| LN | Local National |
| | |
| MCCES | Marine Corps Communication Electronic School |
| MCCSP | Marine Corps Cybersecurity Program |
| MCCYC | Marine Corps Cybersecurity Consortium |
| MCEN | Marine Corps Enterprise Network |
| MCO | Marine Corps Order |
| MCTIMS | Marine Corps Training and Information Management System |
| MEF | Marine Expeditionary Force |
| MOCC | Management, Oversight, and Compliance Council |
| MOS | Military Occupational Specialty |
| MSC | Major Subordinate Command |
| | |
| NICCS | National Initiative for Cybersecurity Careers and Studies |
| NICE | National Initiative for Cybersecurity Education |
| | |
| OPR | Office of Primary Responsibility |
| OS/CE | Operating System / Computing Environment |
| OS/EE | Operating System / Enclave Environment |
| OS/NE | Operating System / Network Environment |
| | |
| PED | Portable Electronic Device |
| PKI | Public Key Infrastructure |
| POTUS | President of the United States |
| | |

| | |
|--------|---|
| RDT&E | Research, Development, Testing & Evaluation |
| | |
| SCI | Sensitive Compartmented Information |
| SECNAV | Secretary of the Navy |
| SIAO | Senior Information Assurance Official |
| SME | Secure Mobile Environment |
| SP | Service Provider |
| | |
| TWMS | Total Workforce Management System |
| | |
| UCMJ | Uniform Code of Military Justice |
| USMC | United States Marine Corps |
| UIP | Unit Inspection Program |
| | |
| VTE | Virtual Training Environment |
| | |
| WAN | Wide Area Network |
| WIP | Workforce Improvement Program |

This page intentionally left blank