



DEPARTMENT OF THE NAVY  
CHIEF OF NAVAL AIR TRAINING  
250 LEXINGTON BLVD SUITE 102  
CORPUS CHRISTI TX 78419-5041

CNATRINST 5239.2  
N6  
19 Mar 12

CNATRA INSTRUCTION 5239.2

Subj: INFORMATION ASSURANCE WORKFORCE (IAWF) TRAINING,  
CERTIFICATION, AND MANAGEMENT PROGRAM

Ref: (a) DoD 8570.01  
(b) DOD 8570.01-M  
(c) SECNAVINST 5239.3B  
(d) SECNAV M-5239.2  
(e) COMNAVCYBERFORINST 5239.1  
(f) SECNAVINST 5239.20  
(g) SECNAV M-5239.1  
(h) OPNAVINST 5239.1C  
(i) SECNAV M-5510.30  
(j) CPFINST 5239.2

Encl: (1) CNATRA IAWF Training and Certification Requirements  
Matrix - By Assigned Classification/Series  
(2) CNATRA IAWF Training and Certification Requirements  
Matrix - Appointed IA Positions  
(3) CNATRA IAWF Training and Certification Requirements  
Matrix - IA Qualification Requirements  
(4) CNATRA IAWF Training and Certification Requirements  
Matrix - OS & CE Certification Guidance

1. Purpose

a. Provide Chief of Naval Air Training (CNATRA) headquarters and subordinate commands the regulations and guidance governing the Department of the Navy (DoN) Information Assurance Workforce (IAWF) Program. References (a) and (b) establish policy and guidance for the training, certification and management of IAWF across the Department the Defense. References (c) through (f) provide direction and guidance for DoN IAWF Management.

b. Establish the CNATRA IAWF Training, Certification and Management Program under the direction of references (c) and (d) and in compliance with references (e) through (j).

2. Objectives

a. Develop a professional Information Technology (IT) workforce with a common understanding of Information Assurance

(IA) concepts and principles, and the skills to effectively prevent and respond to attacks against government information systems and networks.

b. Ensure CNATRA has a competent IT workforce which is appropriately trained and commercially certified in technical and non-technical IA functional areas.

### 3. Applicability

a. This instruction applies to all CNATRA military, civilian and contractor personnel who work to develop, procure, administer or secure classified collateral or unclassified information systems and networks.

b. Military, civilian or contractor personnel who have privileged access to government information systems or have significant administrative IT responsibilities may be considered a part of the IA Workforce without regard to rank/grade, rating/designator/MOS, occupational series, job title, or whether IA duties are performed full-time, part-time or as collateral duty.

### 4. Background

a. To standardize and improve the knowledge and skills of IA professionals across the Department of Defense (DoD), the Services were mandated to implement the Information Assurance Workforce Improvement Program (IA WIP) in accordance with references (a) and (b). The IA WIP requires the Services to identify military and civilian billets with significant IT security responsibilities, identify personnel filling these positions, and ensure they receive specialized training and are commercially certified to perform assigned IA job functions. Policy and implementation guidance for the Department of Navy IA Workforce Program is promulgated in references (d) through (f).

b. The Information Assurance Workforce focuses on the operation and management of IA capabilities for Department of Defense (DoD) information systems (IS) and networks. The IAWF ensures that adequate security measures and established IA policies and procedures are applied to all IS and networks. The IA Workforce training and certification program establishes a baseline of validated knowledge that is relevant, recognized and accepted across the Department of Defense.

5. Roles and Responsibilities

a. All IAWF members are required to be trained and commercially certified. This requirement applies to privileged users and IA staff of: Navy Marine Corps Intranet (NMCI), OCONUS Naval Enterprise Network (ONE-NET); Integrated Shipboard Network System (ISNS), Next Generation Enterprise Network (NGEN), Consolidated Afloat Networks and Enterprise Services (CANES), Program of Record (POR) systems, and Research, Development, Test, and Evaluation (RDT&E) network.

b. All personnel with any level of access to DoD Information Systems (IS) are required to meet security background investigation requirements per reference (b), and IA Awareness Training per Chapter 6 of reference (c). Personnel responsible for engineering, developing, or administering CNATRA IS or providing IA management oversight are additionally required to attain and maintain certifications required for performance of specific duties as outlined in enclosures (1) through (4) of this instruction. CNATRA is required to identify and track positions with IA responsibilities, and personnel performing these IA functions in order to develop and maintain a workforce that is sufficiently educated and trained to assure the security of government networks and information as required by reference (g).

c. All CNATRA Military, Civilian and contractor IAWF personnel are required to attain and maintain levels of training and certification commensurate with assigned and/or appointed duties for the system(s) they access, administer or manage, regardless of occupational specialty - whether the duty is performed as primary or as additional/embedded duty. Manpower positions shall be aligned to applicable IA category and level per reference (e), and documented in applicable personnel and training databases and the Total Workforce Management Services (TWMS) IAWF Module, as required by reference (h). All IA training and certification of CNATRA assigned, attached or contracted personnel shall be tracked until transfer or separation from the command. Certification of IAWF personnel is a condition of employment. Individuals in IA positions not meeting certification requirements within six months of receipt onboard must be reassigned to other duties or released from employment, consistent with applicable law. Individuals not meeting certification requirements may perform those duties under the direct supervision of an appropriately certified individual until certification is attained, only if waived by the Navy Designated Accrediting Authorities (DAA) due to severe operational or personnel constraints. To meet these

requirements, the following responsibilities are assigned per reference (f):

(1) Commanding Officers, Commanders, Officers in Charge, and civilian heads of activities shall:

- (a) Comply with applicable IA policy/guidance;
- (b) Develop a local IA WIP implementation plan;
- (c) Ensure the local IAWF is identified and documented in approved data bases and the TWMS IAWF Module;
- (d) Ensure the local IAWF member is trained, certified and properly qualified;
- (e) Authorize the IA Program Manager to oversee the IA WIP and ensure compliance; and
- (f) Assign manpower, personnel, and training responsibilities to local human resources, administrative, and training officers to carry out IAWF management.

(2) IA Program Manager shall:

- (a) Track and report standard and consistent IAWF data to the next higher authority;
- (b) Provide oversight for IAWF professional's career path and training guidance, on-the-job training, and commercial certification;
- (c) Provide oversight for the command IA WIP, and conduct program reviews to ensure unit level IAWF management compliance; and
- (d) Provide oversight for IA awareness and training programs.

(3) Command IAM shall:

- (a) Work with the immediate superior in the chain of command (ISIC) and Navy IA WIP Offices of Primary Responsibility (OPR) to meet shared IAWF management oversight and compliance responsibilities.
- (b) Ensure service electronic reporting mechanisms are used in order to report consistent data to the ISIC.

(c) Obtain TWMS Security Coordinator privileged access following procedures in reference (h). This access is required to support tracking training and certification status of all assigned IAWF personnel from initial assignment through transfer or separation from the command.

(d) Coordinate with commanders, department heads and supporting manpower offices to ensure all IAWF positions (both military and civilian) are properly identified in the applicable manpower database(s) IAW paragraph 3.2.6 of reference (e).

(e) Validate/verify that all assigned IAWF personnel are matched to IAWF billets and reflected as such in the TWMS IAWF module as required by paragraph 4 of reference (h).

(f) Ensure all IA personnel with privileged access complete a Privileged Access Agreement (PAA).

(g) Ensure all IAT and IAM workforce personnel are designated in writing.

(h) Track IA personnel training and certification against position requirements.

(i) Coordinate with command manpower representatives/administrators, departmental/divisional officers and/or supervisors to ensure IAWF personnel are identified as performing IA responsibilities as primary or as an additional or embedded duty and ensure all required information is properly reflected in the applicable databases.

(j) Coordinate with Command Manpower representative as required to be appraised of command IAWF billet requirements against and alignment with activity manning requirements.

(k) Coordinate with Command Training Officer and administrative representative as required to ensure command IAWF program personnel are in alignment with activity manning requirements.

(l) Ensure a process is in place to ensure all site contracts include the written provision that contractors must hold the appropriate certification IAW Defense Federal Acquisition Regulation Supplement (DFARS) 48 Code of Federal Regulations (CFR) Parts 239 and 252 Record Identification Number (RIN) 0750-AF52 DFARS: IA Contractor Training and Certification (DFARS Case 2006-D023).

(4) IAWF personnel shall:

(a) Comply with IAWF requirements directed in references (a) through (h) by ensuring awareness of individual commercial certification requirements associated with assigned position/appointed duties and taking personal responsibility for individual training, certification and development compliance requirements.

(b) Complete required training/certification within six months of reporting onboard. Reference (b) for training and certification guidance based on assigned/appointed IA duties.

(c) Military personnel reporting onboard will complete a page 13 indicating their understanding of the training/certification requirements associated with their assigned position.

(d) Provide certification certificate and exam grade report(s) to Command Training Officer to ensure IAWF database is updated.

(e) Complete and provide proof of completion of required annual continuing education based on certification requirements.

(5) IS users, including all command military personnel, government employees, contractors, local nationals, foreign or domestic guest researchers, visitors, or associates requiring access to information and or systems shall:

(a) Understand and comply with command IA policies and procedures.

(b) Complete and report awareness and training compliance through their ISIC to the Command Training Officer.

(c) Have a current SAAR-N signed and on file with the Command IAM.

(6) Command Training Officers shall:

(a) Process and submit IAWF certification exam voucher requests to U.S. Navy, Credentials Program Office for approval.

(b) Coordinate and schedule required professional certification training (A+, Network+, Security+, GSLC, CISSP, etc.) when demand necessitates.

(c) Ensure departmental/divisional officers provide each new IAWF individual with a required Personnel Qualification Standards (PQS)/Job Qualification Requirements (JQR) and Individual Training Plan (ITP).

(d) Ensure Individual Training Plans (ITP) are maintained for all IAWF personnel and that ITPs are reviewed and updated to guarantee success of continued learning for all designated IAWF personnel.

(e) Obtain TWMS Training Coordinator privileged access following procedures in reference (h). This access is required to support tracking training and certification status of all assigned IAWF personnel from initial assignment through transfer or separation from the command.

(f) Document and maintain the certification status of IAWF personnel. Ensure all required information is properly reflected in the IAWF database(s).

(g) Track and Report on command IA training (including awareness) and certification programs to Administrative ISIC as required.

(h) Report status of command IAWF to the Chief of Staff at the Staff briefing.

(7) Command Manpower/Administrative Officer shall:

(a) Ensure all IA positions with IA functions are identified by category and level in the site Activity Manpower Document (AMD).

(b) Ensure all civilian IAWF position descriptions are updated to include certification to be held as a condition of employment.

(8) Department Heads shall:

(a) Ensure Personnel in technical category positions maintain certifications, as outlined in enclosure (a) through (c), to retain privileged system access. At a minimum, IAT Level 1 certification is required prior to being authorized unsupervised privileged access.

(b) Ensure all IAWF incumbents and new hires are compliant with IAWF requirements directed in references (a) through (i).

(c) Ensure IAWF personnel who are not appropriately certified within six months of assignment to an IA position, or who fail to maintain their certification status, are not permitted privileged access and/or are submitted for waiver.

## 6. IA Workforce Structure

a. CNATRA designated IAWF personnel are commonly assigned to one of the following IAWF categories: IA Technical (IAT), IA Management (IAM), IA System Architecture and Engineering (IASAE), or Computer Network Defense (CND). IAWF positions may be filled by U.S. Military Officers, Enlisted, or Civilian employees. Certain IAWF duties may also be performed by U.S. Contractors and Foreign National/Local National (FN/LN) personnel under provisions of references (c), (d) and (e) as demonstrated in enclosures (1) and (2) of this instruction:

(1) Basic security clearance requirements and some commonly assigned duties, based upon assigned personnel classifications and series, are identified in enclosure (1). This listing is not all-inclusive but does identify commonly assigned IAWF personnel.

(2) Enclosure (2) provides additional details related to commonly assigned IA duties and identifies overall security clearance requirements, levels of duties commonly assigned by appointment, and personnel who may be authorized to perform these IA functions.

(3) General security clearance and IAWF Training/Certification requirements are identified in reference (b). These requirements are based upon assigned and/or appointed duties, as identified in enclosures (1) and (2).

(4) Baseline certifications presented in reference (d) are based on Appendix 3 of reference (d). Operating System (OS) and Computing Environment (CE) certification guidance for IA Technical (IAT) and Computer Network Defense (CND) duties is provided in Appendix G of reference (e). Flow charts depicting baseline and OS/CE certifications for IAT duties may be found at

the Navy Credentialing Opportunities On-Line (COOL) portal at [https://www.cool.navy.mil/ia\\_documents/ia\\_IAT\\_flow.htm](https://www.cool.navy.mil/ia_documents/ia_IAT_flow.htm). Flow charts for IA Manager (IAM), IA System Architect and Engineer (IASAE), and Computer Network Defense (CND) duties may be accessed by substituting "IAT" in the URL above with IAM, IASAE, or CND as applicable.

(a) IAWF Categories, Specialties and Levels.

(b) Training and Certification.

7. Updates. CNATRA N6 is responsible for required reviews and update of this instruction. All commands may address questions and submit changes to this instruction to N62.

R. L. CURTIN  
Chief of Staff

Distribution: CNATRA Website

CNATRA IAWF Training and Certification Requirements Matrix - By Assigned Classification/Series

Position Held	Security		Technical			Management				Arch & Eng			CND-SP				Civilian	Contractor	Foreign/ Local National (FN/LN)	Notes and References
	IT-I- Critical Sensitive- SSB	IT-II- Non-Critical Sensitive- NACI/NACL	IAT Level I- Computing Environment	IAT Level II- Network Environment	IAT Level III - Enclave	IAM Level I - Computing Environment	IAM Level II - Network Environment	IAM Level III - Enclave	CIO	DAA	IASAE Level I - Computing Environment	IASAE Level II - Network Environment	IASAE Level III - Enclave	Analyst (CND - A)	Infrastructure Support (CND-IS)	Incident Responder (CND-IR)				
Information Assurance Workforce (IAWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment																			NOTE: See Certification Requirements at enclosure (3) for additional details. <b>References:</b> (a) DoD 8570.01-M, IA Workforce Improvement Program, 19 Dec 2005. (b) DoDI 8500.2 "IA Implementation, 6 Feb 2003 (c) SECNAV M-5239.2 DON IA Workforce Management Manual to Support the IA Workforce Improvement Program, May 2009	
<i>Assigned Classifications/Series</i>																				
<b>CIVILIAN</b>																				
2210 - Information Technology (IT) Specialist	X	X							X	X									Y	
0854 - Lead Computer Engineer	X	X																	Y	
0855- Lead Electronics Engineer	X	X																	Y	
1550 - Lead Computer Scientist	X	X																	Y	
<b>CONTRACTORS</b>	X	X	X	X	X									X	X				C	
Foreign or Local National (FN/LN)	X	X																	C	

**Legend**

X level required based on environment and level of responsibility/assigned functions  
 Y Yes - Authorized  
 C Conditional - Based on notes below  
 N No - Not Authorized

CNATRA IAWF Training and Certification Requirements Matrix - Appointed IA Positions

Position Held	Security		Technical			Management				Arch & Eng			CND-SP				Civilian/Contractor			Notes and References	
	IT-I- Critical Sensitive- SSBI	IT-II- Non-Critical Sensitive- NACI/NACLCL	IAT Level I- Computing Environment	IAT Level II- Network Environment	IAT Level III - Enclave	IAM Level I - Computing Environment	IAM Level II - Network Environment	IAM Level III - Enclave	CIO	DAA	IASAE Level I - Computing Environment	IASAE Level II - Network Environment	IASAE Level III - Enclave	Analyst (CND - A)	Infrastructure Support (CND-IS)	Incident Responder (CND-IR)	Auditor (CND-AU)	Manager (CND-SPM)	Civilian		Contractor
Information Assurance Workforce (IAWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment																					<p><b>NOTE:</b> See Certification Requirements at enclosure (3) for additional details.</p> <p><b>References:</b></p> <p>(a) DoD 8570.01-M, IA Workforce Improvement Program, 19 Dec 2005.</p> <p>(b) DoDI 8500.2 "IA Implementation, 6 Feb 2003</p> <p>(c) SECNAV M-5239.2 DON IA Workforce Management Manual to Support the IA Workforce Improvement Program, May 2009</p>
<b>Appointed IA Positions</b>																					
<b>Certifying Authority (CA)</b>																					
Validator	X																	Y	Y	N	No grade or series requirement specified.
Validator Support	X			X	X	X	X											Y	Y	C	No grade or series requirement specified. IATHAM certification levels depend on assigned job functions. FN/ LN- only as authorized/ approved per Ref (b), Table E3. T1 and Ref ©, Para 3.13
Command Information Officer (CIO)	X								X									Y	N	N	Normally military designated rank or grade level comparable to GS 13-15.
IA Program Manager (IAPM)	X							X										Y	N	N	Normally O5 or above or civ equivalent.
Information Assurance Manager (IAM)																					

**Legend**

X level required based on environment and level of responsibility/assigned functions  
 Y Yes - Authorized  
 C Conditional - Based on notes below  
 N No - Not Authorized

Enclave Level IAM	X							X											Y	N	N	Normally military designated rank or grade level comparable to GS 13-15. Recommended fill: 2210 series w/ Security specialty or officer with IA specialty/ sub-specialties.	
Network Level IAM	X							X												Y	C	N	Normally GS 11-14 (or equivalent) level employee or officer with significant security experience. For tactical/ shipboard normally staff NCO/ CPO. Contractors not allowed, except on temporary basis with waiver per Ref (b), Para 18.4.2.
Computing Level IAM		X						X												Y	C	N	No grade restrictions identified. (This is the only IAM job that may be performed on collateral duty basis.) Contractor may hold at IAM Level I only.
Information Assurance Officer (IAO)	X	X		X	X	X	X													Y	C	C	IT, IAM/ IAT, and grade levels based on level of responsibilities stated in appointment letter. Contractors may not perform oversight functions at the Level III environment. FN/ LN- only as authorized/ approved per Ref (b), Table E3. T1 and Ref ©, Para 3.13.
Computer Network Defense- Service Provider (CND-SP)																							See DoD 8570.01-M, Para C11.2.4.3 for requirements that CND-SP specialty personnel must meet prior to deployment to a combat environment.
Incident Management																							
<i>Incident Response IAO/SYS ADM</i>	X	X	X	X											X					Y	Y	N	No grade restrictions specified.
Vulnerability Mgmt	X	X						X	X							X				Y	C	N	No grade restrictions specified. Contractors may not hold the CND- SPM position except with a waiver per Ref (b), Para 1.8.7.6.

CNATRA IAWF Training and Certification Requirements Matrix - IA Qualification Requirements

Qualification Requirements	Security		IA Technical			IA Management				IA System Architect & Engineer			Notes and References
	IT-I- Critical Sensitive- SSBI	IT-II- Non-Critical Sensitive- NACI/NACLCL	IAT Level I	IAT Level II	IAT Level III	IAM Level I	IAM Level II	IAM Level III	CIO	IASAE Level I	IASAE Level II	IASAE Level III	
Information Assurance Workforce (IAWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment													<b>References:</b> (a) DoD 8570.01-M, IA Workforce Improvement Program, 19DEC 2005. (b) DoDI 8500.2, "IA Implementation, 6 Feb 2003. (c) SECNAV M-5239.2, DON IA Workforce Management Manual to Support the IA Workforce Improvement Program, May 2009 <b>NOTE:</b> Certifications identified below are for <b>guidance only</b> and may be adjusted as required to meet command requirements.
Background Investigation			Yes- Level based on Operational Environment	Yes- Level based on Operational Environment	Yes- Level based on Operational Environment	Yes- Level based on Operational Environment	Yes- Level based on Operational Environment	IT-1- Critical Sensitive: SSBI for U.S. Military, Civilian and Contractor. IT-2- Non-Critical Sensitive: NACI for U.S. Civilian: NACLCL fo U.S. Military and contractor					
Required Experience	X	X	Normally 0 to 5 or more yrs in IA tech or related field	Normally 0 to 5 or more yrs in IA tech or related field	Normally 0 to 5 or more yrs in IA tech or related field	Usually entry level, 0 to 5 or more yrs mgmt experience	Usually at least 5 or more yrs mgmt experience	Usually at least 10 or more yrs mgmt experience		Usually entry level, 0 to 5 yrs IASAE experience	Usually at least 5 or more yrs of IASAE experience	Usually at least 10 or more yrs of IASAE experience	
Initial Training Required	X	x	Classroom, distributive, blended, Gov or Commercial provider	Executive Level IA Course	Classroom, distributive, blended, Gov or Commercial provider	Classroom, distributive, blended, Gov or Commercial provider	Classroom, distributive, blended, Gov or Commercial provider						

OJT Evaluation			Yes- (for initial position)	Yes- (for initial position)	Yes- (for initial position)	No	No	No	No	No	No	No	
Certification Completion Requirements (from DoD approved List of Baseline Certifications)	X	X	IA Certification within 6mo.	IA Certification within 6mo.	IA Certification within 6mo.	IA Certification within 6mo.	IA Certification within 6mo.	IA Certification within 6mo.		IA Certification within 6mo.	IA Certification within 6mo.	IA Certification within 6mo.	6- MONTH REQUIREMENT APPLIES TO BASELINE CERTIFICATION. CE/ OS Certifications may require additional time.
DoD Approved List of Baseline Certifications (per DoD 8570.01-M, Appendix 3)	X		A+ Network+ SSCP	GSEC Security+ SCNP SSCP	CISA GCIH GSE SNCA CISSP (OR Associate)	CAP GISF GSLC Security +	CAP GSLC CISM CISSP (or Associate)	GSLC CISM CISSP ( or Associate)		CISSP (or Associate)	CISSP (or Associate)	CISSP - ISSEP CISSP- ISSAP	Go to Navy COOL website. <a href="https://www.cool.navy.mil/ia_documents/ia_iat_flow.htm">https://www.cool.navy.mil/ia_documents/ia_iat_flow.htm</a> for up-to-date, detailed Navy IAT certification options. For access to IAM, IASAE or CND info, replace IAT in the URL above with iam,iasae or cnd.
Computing Environment (CE)/ Operating System (OS) Cert Required	x		Yes	Yes	Yes	No	No	No	No	No	No	No	CE/ OS certification requirements are based on duties assigned in privileged access authorization letter. (See OS-CE Cert Guidance worksheet at next tab.)
Maintain Certification Status	X	x	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Maintenance requirements are specific to each required certification.
Continuous Education or Sustainment Training			Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Continous Professional Education (CPE) or sustainment training is rrequired based on each required certification. See reference (c), paragraph 4.3.3 for CPE examples.
Appointment, in writing, to include statement of IA responsibilities and training requirements per reference (c). Paragraph 2.4.1.	x	X	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	Yes	See Reference (c) Appendix C for sample based on IAM appointment.
Sign Privileged Access Statement	X	X	Yes	Yes	Yes	N/A	N/A	N/A	N/A	N/A	N/A	N/A	

CNATRA IAWF Training & Certification Requirements Matrix - OS & CE Certification Guidance

OS/ CE Certifications	Information Assurance Technical (IAT)										Computer Network Defense Service Provider (CND-SP)			Notes and References	
	IAT Level I		IAT Level II				IAT Level III				CND-A ANALYST	CND- IS INFRASTRUCTURE SUPPORT	CND-IR INCIDENT RESPONDER		CND-AU AUDITOR
Information Assurance Workforce (IAWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment	DESK TOP SUPPORT	NETWORK INFRASTRUCTURE	DOMAIN INFRASTRUCTURE	NETWORK INFRASTRUCTURE	DATABASE SUPPORT	WEB SERVICE	DOMAIN INFRASTRUCTURE	NETWORK INFRASTRUCTURE IAM Level II	DATABASE SUPPORT	WEB SERVICE				SOFTWARE Developer	
Certified Internet Web Professional															
CIW-A						X**									
CIW-P										X**			X	X	
CIW-MA										X**		X	X	X	
CISCO															
CCNA				X								X	X		
CCENT		X		X								X	X		
CAWLFS				X									X		
CCDP													X		

**NOTES:**  
\*Certification exams/ tracks are no longer offer but are still valid and will be required to support such Computing Environments per reference (a).  
\*\*Highly recommend coupling with server-based certification per reference (a).  
**References:**  
(a) SECNAV M5239.2, DON IA Workforce Management Manual, Appendix G  
(b) Navy Credentialing Opportunities on-line (COOL) Portal (<https://www.cool.navy.mil/>)

<i>CCNP</i>								X						X	X	
<i>CCDE</i>								X						X	X	
<i>CAWLDs</i>								X						X	X	
<b>COMP T/A</b>																
Linux+	X		X		X	X			X	X	X	X	X	X	X	
server+					X	X							X			
<b>HP</b>																
CSA	X				X	X			X	X	X	X	X			
CSE							X							X	X	
<b>IEEE</b>																
CSDP											X**			X	X	