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

CNATRAINST 5239.2A
N6
26 Nov 2014

CNATRA INSTRUCTION 5239.2A

Subj: CYBERSECURITY WORKFORCE 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 CSWF Training and Certification Requirements Matrix – By Assigned Classification/ Series
(2) CNATRA CSWF Training and Certification Requirements Matrix – Appointed CS Positions
(3) CNATRA CSWF Training and Certification Requirements Matrix – CS Qualification Requirements
(4) CNATRA CSWF Training and Certification Requirements Matrix – Operating System (OS) and Computing Environment (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) Cybersecurity Workforce (CSWF) Program. References (a) and (b) establish policy and guidance for the training, certification and management of CSWF across the Department the Defense. References (c) through (f) provide direction and guidance for DoN CSWF Management.

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

2. Cancellation. CNATRAINST 5239.2

3. Objectives

a. Develop a professional Information Technology (IT) workforce with a common understanding of Cybersecurity (CS) 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 CS functional areas.

4. Applicability

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

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

5. Background

a. To standardize and improve the knowledge and skills of CS professionals across the Department of Defense (DoD), the Military Services were mandated to implement the Cybersecurity Workforce Improvement Program (CS WIP) in accordance with references (a) and (b). The CS 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 CS job functions. Policy and implementation guidance for the DoN CS WIP is promulgated in references (d) through (f).

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

6. Roles and Responsibilities

a. All CSWF members are required to be trained and commercially certified. This requirement applies to privileged users and CS staff of: Navy Marine Corps Intranet (NMCI), Outside Contiguous United States (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 IS are required to meet security background investigation requirements per reference (b), and CS Awareness Training per Chapter 6 of reference (c). Personnel responsible for engineering, developing, or administering Chief of Naval Air Training (CNATRA) IS or providing CS 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 N6 is required to identify and track positions with CS responsibilities, and personnel performing these CS 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 contract CSWF 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 CS category and level per reference (e), and documented in applicable personnel and training databases and the Total Workforce Management Services

(TWMS) CSWF Module, as required by reference (h). All CS training and certification of CNATRA assigned, attached or contracted personnel shall be tracked until transfer or separation from the command. Certification of CSWF personnel is a condition of employment. Individuals in CS 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 CS policy/guidance;

(b) Develop a local CS WIP implementation plan;

(c) Ensure the local CSWF is identified and documented in approved data bases and the TWMS CSWF Module;

(d) Ensure the local CSWF member is trained, certified and properly qualified;

(e) Authorize the Cybersecurity Program Manager to oversee the CS WIP and ensure compliance; and

(f) Assign manpower, personnel, and training responsibilities to local human resources, administrative, and training officers to carry out CSWF management.

(2) CS Program Manager shall:

(a) Track and report standard and consistent CSWF data to the next higher authority;

(b) Provide oversight for CSWF professional’s career path and training guidance, on-the-job training, and commercial certification;

(c) Provide oversight for the command CS WIP, and conduct program reviews to ensure unit level CSWF management compliance; and

(d) Provide oversight for CS awareness and training programs.

(3) Command Information Assurance Manager (IAM) shall:

(a) Work with the immediate superior in the chain of command (ISIC) and Navy CS WIP Offices of Primary Responsibility (OPR) to meet shared CSWF 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 training and certification tracking status of all assigned CSWF personnel from initial assignment through transfer or separation from the command.

(d) Coordinate with commanders, department heads and supporting manpower offices to ensure all CSWF 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 CSWF personnel are matched to CSWF billets and reflected as such in the TWMS CSWF module as required by paragraph 4 of reference (h).

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

(g) Ensure all Information Assurance Technician (IAT) and Information Assurance Managerial (IAM) workforce personnel are designated in writing.

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

(i) Coordinate with command manpower representatives/administrators, departmental/divisional officers and/or supervisors to ensure CSWF personnel are identified as performing CS 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 CSWF billet requirements against and alignment with activity manning requirements.

(k) Coordinate with Command training officer and administrative representative as required to ensure command CSWF 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: Information Assurance Contractor Training and Certification (DFARS Case 2006-D023).

(4) CSWF personnel shall:

(a) Comply with CSWF 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. See reference (b) for training and certification guidance based on assigned/appointed CS duties.

(c) Military personnel reporting onboard will complete 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 CSWF 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 CS 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 CSWF 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 CSWF individual with a required Personnel Qualification Standards (PQS)/Job Qualification Requirements (JQR) and Individual Training Plan (ITP).

(d) Ensure ITPs are maintained for all CSWF personnel and that ITPs are reviewed and updated to guarantee success of continued learning for all designated CSWF personnel.

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

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

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

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

(7) Command Manpower/Administrative Officer shall:

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

(b) Ensure all civilian CSWF 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 enclosures (1) through (3). Certifications must be maintained in order to retain privileged system access. At a minimum, IAT Level 1 certification is required prior to being authorized unsupervised privileged access.

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

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

7. CS Workforce Structure: CNATRA designated CSWF personnel are commonly assigned to one of the following CSWF categories: IAT, IAM, IA System Architecture and Engineering (IASAE) or Computer Network Defense (CND). CSWF positions may be filled by U.S. Military Officers, Enlisted, or Civilian employees. Certain CSWF 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:

a. 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 CSWF personnel.

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

c. General security clearance and CSWF 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).

d. Baseline certifications presented are based on Appendix 3 of reference (d). Operating System (OS) and Computing Environment (CE) certification guidance for 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/usn/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.

8. 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.

9. Records Management. Records created as a result of this instruction, regardless of media and format shall be managed per SECNAV Manual 5210.1 of January 2012.

D. M. EDGECOMB
Chief of Staff

Distribution:
CNATRA Website
CNATRA SharePoint

CNATRA CSWF TRAINING AND CERTIFICATION REQUIREMENTS MATRIX – BY ASSIGNED CLASSIFICATION/SERIES

Position Held	Security		Technical			Management					Arch & Eng			CND-SP								Notes and References
Cybersecurity Workforce (CSWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment	IT-I- Critical Sensitive- SSBI	IT-II- Non-Critical Sensitive- NACI/NACLC	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	Foreign/Local National (FN/LN)	**NOTE**: See Certification Requirements at enclosure (3) for additional details. **References:** (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 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
Assigned Classifications/Series																						
CIVILIAN																						
2210 - Information Technology (IT) Specialist	X	X							X	X									Y			
0343 – Management/ Program Analyst	X	X																	Y			
1083 – Technical Writer/Editor	X	X																	Y			
0854 - Lead Computer Engineer	X	X																	Y			
0855- Lead Electronics Engineer	X	X																	Y			
1550 - Lead Computer Scientist	X	X																	Y			

CONTRACTORS	X	X	X	X	X										X	X				C		Restrictions apply to some positions/ functions reflected under Appointed CS Positions, below.
Foreign or Local National (FN/LN)	X	X																			C	FN/ LN require security clearance and authorization approval IAW Ref (B), Table E3. T1 and Ref ©, Para 3.13

CNATRA CSWF TRAINING AND CERTIFICATION REQUIREMENTS MATRIX – APPOINTED CS POSITIONS

Position Held	Security		Technical			Management					Arch & Eng			CND-SP								Notes and References
Cybersecurity Workforce (CSWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment	IT-I- Critical Sensitive- SSBI	IT-II- Non-Critical Sensitive- NACI/NACLC	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	Foreign/Local National (FN/LN)	**Note:** See Certification Requirements at enclosure (3) for additional details. **References:** (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 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
Appointed CS Positions																						
Certification Authority (CA)																						
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.
CS Program Manager (IAPM)	X							X											Y	N	N	Normally 05 or above or civ equivalent.
Information Assurance Manager (IAM)																						
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

																					CS 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																					
Incident Response IAO/SYS ADM	X	X	X	X											X			Y	Y	N	No grade restrictions specified.
Vulnerability Management	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 CSWF TRAINING AND CERTIFICATION REQUIREMENTS MATRIX – CS QUALIFICATION REQUIREMENTS

Qualification Requirements	Security		IA Technical			IA Management				IA System Architect & Engineer			Notes and References
Cybersecurity Workforce (CSWF) Baseline Position Authorizations and Fill Requirements By Position and Duty Assignment	IT-I- Critical Sensitive- SSBI	IT-II- Non-Critical Sensitive- NACI/NACLC	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	**References:** (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 **Note:** Certifications identified below are for **guidance only** 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	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: NACLC for U.S. Military and contractor
Required Experience	X	X	Normally 0 to 5 or more yrs. in CS tech or	Normally 0 to 5 or more yrs. in CS tech or	Normally 0 to 5 or more yrs. in CS tech or	Usually entry level, 0 to 5 or more yrs. managemen	Usually at least 5 or more yrs. managemen	Usually at least 10 or more yrs. managemen		Usually entry level, 0 to 5 yrs. IASAE experience	Usually at least 5 or more yrs. of IASAE	Usually at least 10 or more yrs. of IASAE	

			related field	related field	related field	t experience	t experience	t experience			experience	experience	
Initial Training Required	X	X	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government or Commercial provider	Executive Level CS Course	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government or Commercial provider	Classroom, distributive, blended, Government 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	CS Certification within 6mo.	CS Certification within 6mo.	CS Certification within 6mo.	CS Certification within 6mo.	CS Certification within 6mo.	CS Certification within 6mo.		CS Certification within 6mo.	CS Certification within 6mo.	CS Certification within 6mo.	6- MONTH REQUIRMENT 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: https://www.cool.navy.mil/ia_documents/ia_iat_flow.htm 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	Continuous Professional Education (CPE) or sustainment training is required based on each required certification. See reference (c), paragraph 4.3.3 for CPE examples.
Appointment, in writing, to include statement of CS 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	

COMPACFLT CSWF TRAINING AND CERTIFICATION REQUIREMENTS MATRIX – OS AND 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									
Cybersecurity Workforce (CSWF) 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 INFRASTRUCTUREIAM Level II	DATABASE SUPPORT	WEB SERVICE	SOFTWARE Developer	CND-A ANALYST	CND- IS INFRASTRUCTURE SUPPORT	CND-IR INCIDENT RESPONDER	CND-AU AUDITOR	**Note:***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/)
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			
CCNP								X						X	X	

Enclosure (4)

CCDE								X						X	X	
CAWLDS								X						X	X	
COMP T/A																
Linux+	X		X		X	X			X	X	X	X	X	X	X	
server+					X	X							X			
HP																
CSA	X				X	X			X	X	X	X	X			
CSE							X							X	X	
IEEE																
CSDP											X			X	X	

Enclosure (4)