**DEPARTMENT OF THE NAVY**
COMMANDER NAVY RESERVE FORCE
1915 FORRESTAL DRIVE
NORFOLK, VIRGINIA 23551-4615

COMNAVRESFORINST 5239.4A
N64
27 Feb 2014

COMNAVRESFOR INSTRUCTION 5239.4A

From: Commander, Navy Reserve Force

Subj: CYBERSECURITY TRAINING, CERTIFICATION AND WORKFORCE MANAGEMENT

Ref: (a) DoD Directive 8570.01 of 15 August 2004
(b) DoD 8570.01-M, Information Assurance Workforce Improvement Program, 12 January 2013
(c) SECNAV M-5239.2, Department of the Navy Information Assurance Workforce Management Manual
(d) SECNAVINST 5239.20
(e) COMNAVCYBERFORINST 5239.1

Encl: (1) Cybersecurity Workforce Determination Guide
(2) Waiver Letter Template
(3) Cybersecurity Workforce Certification List
(4) Sample IAM/IAO Letter of Designation

1. Purpose. To promulgate Cybersecurity (CS) training plan, certification guidelines and Cybersecurity Workforce (CSWF) management for personnel assigned to such positions per references (a) through (e). To establish policy and assign responsibilities for Department of Defense (DoD) CS training, certification and workforce management. This instruction is a complete revision and should be reviewed in its entirety.

2. Cancellation. COMNAVRESFORINST 5239.4.

3. Background. In today's network-centric environment, CS is a paramount concern. To mitigate risks associated with network operations, personnel with specific levels of Information Technology (IT) responsibility within the Reserve Force structure must be adequately trained to execute their functions. Navy leadership has established training levels based on an individual's role at the enclave, network or computing level. Additionally, they provide guidance and detail procedures for the training, certification and management of the DoD workforce conducting CS functions in assigned duty positions.

4. Scope. All CSWF personnel identified within this instruction are required to meet the minimum levels of training and certification for the required system they administer, regardless of occupational specialty or whether the duty is performed as primary or an additional/embedded duty. Positions will be aligned to a CS category (Information Assurance Technician/Information Assurance Manager (IAT/IAM) and level (I, II or III), documented in the appropriate database(s) and tracked until transfer or separation from the command. Enclosure (1) is provided as a guide to determine which category and level personnel will generally be billeted based on assigned department and division.

a. Designated CSWF personnel in the Reserve Force may include officers, U.S. Government civilian employees, U.S. Contractors and enlisted Sailors, normally Information Technicians. The functions performed by CSWF personnel may be accomplished by any rate.

(1) Enlisted Sailors possessing the following Naval Enlisted Classification (NEC) codes are designated as CSWF personnel. Personnel with 0000 NEC or other NECs not referenced here, but assigned to work on a system may also be a member of the CSWF depending on their responsibilities and level of access granted: 2710, 2720, 2735, 2779, 2780, 2781, 2735, 2379 and 2791. This applies to Full Time Support (FTS), Selected Reservist and Information Technicians (ITs).

(2) Officers possessing the following designators are designated as CSWF personnel: 1207 FTS Officers with P or Q coded IT subspecialty and currently filling an N6 billet, 182X and 181X Reserve Officers. Officers not listed above may be part of the CSWF, depending on their role and assigned billet. Officers assigned to N6 at Echelons II, III and IV are included in the CSWF.

(3) U.S. Government civilian employees possessing the 2210 series designator are designated as CSWF personnel. Existing Personnel Job Descriptions (PD) shall include a condition of employment statement reflecting the appropriate certification for a position. Job PDs to new employees shall contain the condition of employment requirement to obtain and maintain the appropriate suitability and commercial certification(s) for the job.

(4) U.S. Contractors are required to maintain CSWF category and level commensurate to the level of access for the system they support and/or manage as defined within this instruction. Job offers to new contractors shall contain the condition of employment requirement to obtain and maintain the appropriate suitability and commercial certification(s) for the job.

b. In addition to the personnel identified within paragraph 3a, only personnel assigned to CS positions are required to fulfill the requirements for the CSWF. Personnel with local workstation only access (are able to login to workstation only and not privileged domain level access) are required to maintain an IAT Level I certification. Personnel who administer multiple systems are required to maintain an IAT Level II certification. Personnel who maintain an enclave (e.g., unclassified and classified) must maintain an IAT Level III certification. Supervisors who oversee the maintenance of IATs must maintain an IAM Level II certification. The Commander, Navy Reserve Forces Command (COMNAVRESFORCOM) (Echelon III) IAM, is required to maintain an IAM Level III certification.

c. Personnel performing the following assigned responsibilities are included in this policy:

(1) Work closely with data owners, information system owners and users to ensure secure use and operation of information systems and networks.

(2) Ensure rigorous application of CS policies, principles and practices in the delivery of all IT services.

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

(4) Identify CS requirements as part of the IT acquisition development process.

(5) Assess and implement identified corrections (e.g., system patches and fixes) associated with technical vulnerabilities as part of the CS Vulnerability Management Program.

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

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

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

(9) Managers and supervisors of IAT personnel.

d. CSWF categories and levels do not necessarily correlate to civilian grades, military ranks or any specific occupational classification standard.

e. Due to various command sizes and compositions, Echelon V Navy Operational Support Centers may not have an CSWF member assigned. CS functions will be performed by a collateral duty command Information Assurance Officer (IAO), who will report directly to the Echelon IV Regional IAM. IAOs must be designated in writing or stated in the Command Collateral Duty List, per enclosure (4), but are not considered part of the CSWF. Therefore, IAOs are not required to earn commercial certifications, but are encouraged to attend training to better perform their collateral duty CS tasks.

f. For additional information on the functions of the various IAM/IAT levels, refer to chapters 3 and 4 of reference (b). Enclosure (1) contains the minimum expected CSWF assignments at COMNAVRESFORCOM Echelons II through V. Commanders at Echelons IV and V are required to work with their command IAM and Training Officer in assigning command CSWF members and tracking required certifications.

5. Action. CSWF training and certification must be maintained at a level corresponding to the system(s) administered. Personnel designated as IAT or IAM will complete required Navy Knowledge Online courses or attend professional classroom training and obtain applicable commercial certifications. All personnel must complete the requirements associated with their level of responsibility. Enclosures (2) and (3) are provided to assist leadership with a reference to determine CS category, workforce personnel shall be placed in (IAT/IAM).

a. COMNAVRESFORCOM preferred certification lists:

(1) IAT Certifications.

(a) Level I - A+ or Network+, plus an Operating System (OS)/Computing Environment (CE) training certificate.

(b) Level II* - Security+, plus an OS/CE training certificate.

(c) Level III* - Global Security Essential Certification (GSEC), Certified Information Systems Security Professional (CISSP) or CompTIA Advanced Security Practitioner (CASP), plus an OS/CE training certificate.

*IAT certifications are cumulative; for example, to achieve IAT Level III, a CSWF member must complete requirements of Level I and II.

(2) IAM Certification List:

(a) Level I* - Security+.

(b) Level II/III - Global Security Leadership Certification (GSLC), CISSP or CASP.

*IAM certifications are not cumulative; for example, if an employee has completed GSLC and is assigned IAM Level II, the employee does not need to complete Security+ to comply with CSWF requirements.

b. Note the above certifications do not constitute the only path to achieve required IAT/IAM level. Enclosure (3) contains a comprehensive list of possible certifications to achieve various levels.

c. In addition to certifications, military and civilian Information Assurance Workforce (IAWF) members must complete the following requirements to attain the required level:

(1) Additional IAT requirements:

(a) Military must complete CS Personal Qualification Standards (PQS).

(b) Civilians must complete CS Job Qualification Requirements (JQR)/On the Job Training (OJT).

(c) Complete Privileged Access Agreement (PAA), if applicable.

(2) Additional IAM requirements:

(a) Military must complete CS PQS.

(b) Civilians must complete CS JQR/OJT.

(c) Current IAM/IAO command designation letter.

d. Individuals in CS positions must meet certification requirements within 6 months of reporting onboard. If certification requirements are not met within this timeframe a waiver may be submitted to the Navy Designated Approving Authorities. A waiver may be granted due to operational or personnel constraints. A waiver letter template is available in enclosure (2).

e. Based on the Department of the Navy's (DON) policy, COMNAVRESFORCOM will fund a maximum of three attempts to successfully pass a certification exam. CSWF members may apply for exam vouchers online at: www.cool.navy.mil. Additionally, COMNAVRESFORCOM will fund CSWF required courses on a case-by-case basis; all efforts should be made to fund boot camps and courses at the command level.

6. Responsibility

a. Commander, Navy Reserve Force (COMNAVRESFOR) Chief Information Officer (CIO) will:

(1) Ensure the Navy Reserve Force maintains a trained and qualified CSWF per references (a) through (d).

b. COMNAVRESFOR IAM will manage the Reserve Force CSWF program.

c. Echelon IV IAMs/COMNAVRESFORCOM (N6) Officers will:

(1) Track CSWF requirements within their region.

(2) Request and maintain Total Workforce Management Services (TWMS) access as IAM/Security Coordinator role, with access to all subordinate Unit Identification Codes.

d. Military and Civil Service CSWF Personnel will:

(1) Coordinate with the Training Officer to review and update records with certification status. If lacking specific certifications for a position, develop an Individual Development Plan (IDP) and schedule required boot camps or courses to attain certification within a 6 month window.

(2) Provide certification exam grade report to Training Officer to ensure CSWF database in TWMS is updated.

e. The Command IAM(s) will:

(1) Obtain and maintain an appropriate level IAM certification, per enclosure (1).

(2) Ensure all IAT and IAM Workforce personnel are designated in writing upon receipt of notification from Training Officer, that an individual passed the appropriate commercial certification examination.

(3) Conduct random Quality Assurance audit of the CSWF program to ensure compliance with established policy.

(4) Ensure all CS personnel with privileged access complete a PAA.

(5) Maintain current repository of all DON CIO, Chief of Naval Operations (CNO) (N6), Commander, Naval Network Warfare Command (NAVNETWARCOM) and Commander, Navy Cyber Forces (COMNAVCYBERFOR) official messages, policy and instructions relating to IAWF management.

(6) Ensure proper oversight structure is in place which permits management of the CS training program to include Training Officer, supervisors of IATs and personnel with privileged access, Computer Network Defense, Certification and Accreditation and all IA professionals.

(7) Ensure compliance with this instruction and all higher DON instructions relevant to CSWF.

f. Echelon V Command IAOs will:

(1) Report to higher Echelon IAM on all CS related incidents.

(2) Be familiar with all DON CIO, CNO N6, NAVNETWARCOM and COMNAVCYBERFOR official messages, policy, and instructions relating to CS. Create a culture of compliance to governing documents within the organization.

(3) As applicable, manage local CS related processes and procedures.

g. Training Officer(s) will:

(1) Coordinate with Command Manpower representative 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 CSWF database(s) per references (a) through (e).

(2) Coordinate and schedule required professional training (A+, Network+, Security+, GSLC, CISSP, CASP etc.).

(3) Report DoD component training (including awareness) and certification programs to administrative Immediate Superior In Charge, as required.

(4) Report status of command CSWF to chain of command.

h. Command Manpower representative will:

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

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

(3) Coordinate with the Training Officer as required to ensure command CSWF program personnel are in alignment with activity manning requirements.

i. The Administrative Officer will ensure all civilian CSWF position descriptions are updated, to include certification to be held as a condition of employment.

j. The Human Resources Officer will ensure PDs contain proper condition of employment statement requiring the appropriate certification for position.

k. The Contracting Officer will ensure contracts contain proper conditions of employment statement requiring the appropriate certification for position.

l. COMNAVRESFORCOM (N68) Division Director will liaise with COMNAVRESFORCOM (N7) and (N8) to fund CSWF training courses. Funding is limited to those billets and positions which require training and certifications per enclosure (1). The Training Officer will outline funding requirements with each fiscal year and keep COMNAVRESFORCOM (N68) informed of financial status with contracted training courses.

m. Department Heads and Division Directors will:

(1) Ensure personnel in technical category positions maintain certifications, as required by the certifying provider, to retain privileged system access. IAT Level I certification is required prior to being authorized unsupervised privileged access.

(2) Ensure personnel who are not appropriately certified within 6 months of assignment to a position or who fail to maintain their certification status are not permitted privileged access.

(3) Assign appropriately trained and certified personnel to CS positions.

(4) Ensure all incumbents and new hires are trained, certified and recertified as part of the CSWF.

n. Subordinate Echelon IV and V commands will follow all guidelines for compliance with CSWF requirements promulgated in references (a) through (e). Echelon IV command CSWF programs are subject to inspection by higher authority.

7. Review and Update. The COMNAVRESFORCOM IAM (N64) is responsible for the annual review and update of this instruction.

8. Forms. The following forms are available for download on the Navy Reserve Headquarters Forms web sites:

a. COMNAVRESFORCOM Cyber Security Workforce (CSWF) Determination Aid for Cybersecurity Technical Assessment Questionnaire, NAVRES 5239/1, (Rev 2-14.)

b. COMNAVRESFORCOM CSWF Determination Aid for Cybersecurity Management Assessment Questionnaire, NAVRES 5239/2, (Rev 2-14.)

B. P. CUTCHEN
Deputy

Distribution:
Electronic Copy via COMNAVRESFOR Web site
https://www.navyreserve.navy.mil

# Cybersecurity Workforce Determination Guide

## Echelon II/III Billets

- N6 Information Technology
  - Chief Information Officer - IAM Level III
  - Force Information Assurance Manager (IAM) - IAM Level III
  - N6 Deputy Chief of Staff/Chief Technology Officer - IAM Level III
  - Assistant N6 Deputy Chief of Staff - IAM Level I
  - Deputy Chief Information Officer for Cybersecurity and Infrastructure - IAM Level II
  - N63 Operations Division Director - IAM Level I
  - N64 Information Assurance Officer - IAM Level II
  - Division Directors/Asst Division Directors - IAM Level I
  - Information Technician's with 27xx or 23xx series NEC(s) - IAT Level II
  - N64 Cybersecurity Division Personnel - IAT Level II
  - Personnel with privileged network access, per reference (a) and enclosures (2) or (3)

- N1 Manpower and Personnel
  - Not required except for Information Technicians with 27xx or 23xx series NEC(s) - IAT Level 1

- N2 Intelligence/Information Warfare
  - Not required

- N3 Operations
  - Information Technicians with 27xx or 23xx series NEC(s) IAT Level I

- N4 Logistics
  - Not required

- N5 Plans and Policy
  - Not required

- N7 Training
  - Not required

- N8 Finance and Accounting
  - Not required

Echelon IV Billets

- N6 Information Technology
  - Department Head assigned to the N6 ADP PLANS/ACOS Billet - IAM Level II
  - Information Technicians with 27xx or 23xx series NEC(s) - IAT Level II
  - Personnel with privileged network access, per reference (e), page 5, paragraph 3e.

Echelon V/VI Billets:

- Information Technicians with 27xx or 23xx series NEC(s) - IAT Level II

Waiver Letter Template

(Official Letterhead)

SSIC
Code/Serial #
Date

From: Activity head, name of activity, location when needed
To: Title, name of activity (Code), location when needed (COMNAVNETWARCOM)

Via: (1) Commander, Navy Reserve Force, Chief Information Officer
(2) Commander, Navy Reserve Forces Command (N6)
(3) Immediate Superior in Command

Subj: CYBERSECURITY WORKFORCE WAIVER REQUEST ICO RANK, NAME

Ref: (a) Navy Telecommunications Directive 02-11 Information Assurance Workforce Waiver Process
(b) DoD Manual 8570.01-M of 19 December 2005
(c) SECNAVINST 5239.20
(d) COMNAVCYBERFORINST 5239.1

1. Per reference (a), request a 6 month waiver for (rank and name) to all certification requirements identified in references (b) through (d). (Rank and Name) currently fills the (job) billet at (command) on a (full-time/part-time) basis and meets the criteria of a (Level III/II/I) Information Assurance Manager. Please find amplifying information below.

a. Date assigned to this position:

b. Certifications required for position:
Security+/GSLC/CISSP

c. Individual Development Plan (IDP): (State plan to achieve certification, course date and continuing education plans).

Subj: CYBERSECURITY WORKFORCE WAIVER REQUEST ICO RANK, NAME

d. Summary of Duties:

e. Rationale for non-compliance to date:

f. Operational impact if waiver is denied:

NAME OF SIGNER
By direction

Enclosure (2)

# Cybersecurity Workforce Certification List

## IAT Level I

One or more of the CS Certs

- COMPTIA A+ Certification
- COMPTIA Network+ Certification
- System Security Certified Practitioner (SSCP)
- COMPTIA Security+ Certification
- Certified Information Systems Security (CISSP)
- Certified Information Security Auditor (CISA)
- GIAC Security Essentials Certification (GSEC)
- Security Certified Network Professional (SCNP)
- Security Certified Network Architect (SCNA)
- GIAC Security Expert (GSE)

AND: One or more OS Certs

- CCNA Certification
- CCNP Certification
- LINUX+ Certification
- HP Certified Systems Administrator
- Microsoft Certified Desktop Support Technician (MCDST)
- Microsoft Certified Professional (MCP) (EXAM 70-270)
- Microsoft Certified Systems Engineer - Server 2003 (MCSE)
- Microsoft Certified Systems Administrator - Server 2003 (MCSA)
- Microsoft Certified Systems Administrator - Windows 2000 (MCSA)
- Microsoft Certified Systems Engineer - Windows 2000 (MCSE)
- Windows 7 or current

For military and civilian personnel, a training certificate for a valid OS/CE course satisfies the requirement. Contract personnel must fulfill obligations outlined in contract and attain OS/CE commercial certification.

## IAT Level II

One or more of the CS Certs

- GIAC Security Essentials Certification (GSEC)
- COMPTIA Security+ Certification
- Security Certified Network Professional (SCNP)
- System Security Certified Practitioner (SSCP)
- Certified Information Systems Security (CISSP)
- Certified Information Security Auditor (CISA)
- Security Certified Network Architect (SCNA)
- GIAC Security Expert (GSE)

AND: One or more OS Certs

- CCNP Certification
- LINUX+ Certification
- HP Certified Systems Administrator
- Microsoft Certified Systems Engineer - Server 2003 (MCSE)
- Microsoft Certified Systems Administrator - Server 2003 (MCSA)
- Microsoft Certified Systems Engineer - Windows 2000 (MCSE)
- Microsoft Certified Systems Administrator - Windows 2000 (MCSA)
- Windows 7 or current

For military and civilian personnel, a training certificate for a valid OS/CE course satisfies the requirement. Contract personnel must fulfill obligations outlined in contract and attain OS/CE commercial certification.

## IAT Level III

One or more of the CS Certs

- Certified Information Security Auditor (CISA)
- GIAC Security Expert (GSE)
- Security Certified Network Architect (SCNA)
- Certified Information Systems Security (CISSP)
- GIAC Certified Incident Handler (GCIH)
- System Security Certified Practitioner (SSCP)

AND: One or more OS Certs

- CCNP Certification
- LINUX+ Certification
- HP Certified Systems Administrator
- Microsoft Certified Systems Engineer - Server 2003 (MCSE)
- Microsoft Certified Systems Engineer - Windows 2000 (MCSE)
- Windows 7 or current

IAM Level I

One or more of the CS Certs

- COMPTIA Security+ Certification
- GIAC Security Leadership Certification (GSLC)
- GIAC Information Security Fundamental (GISF)
- Certification & Accreditation Professional (CAP)

IAM Level II/III

One or more OS Certs

- Certified Information Systems Security (CISSP)
- GIAC Information Security Fundamental (GISF)
- GIAC Security Leadership Certification (GSLC)
- Certified Information Security Manager (CISM)
- Certification & Accreditation Professional (CAP)
- CompTIA Advance Security Practitioner (CASP)

Sample IAM/IAO Letter of Designation

(Official Letterhead)

SSIC
Code/Serial #
Date

From: Activity head, name of activity, location when needed
To: Rank First name, Last name

Subj: APPOINTMENT AS INFORMATION ASSURANCE (MANAGER/OFFICER)

Ref: (a) DoD Instruction 8500.1, of 24 Oct 2002
(b) DoD Instruction 8500.2, of 6 Feb 2003
(c) CJCS Instruction 6510.01D, of 15 Jun 2004
(d) CJCS M-6510.01, Defense-in-Depth: Information Assurance and Computer Network Defense, 25 March 2003, W/CH 3, 8 March 2006
(e) DoD 5200.2R, Personnel Security Program, January 1987
(f) DoD 5200.1-R DoD Information Security Program Regulation, January 1997
(g) DoD Instruction 5200.40, DoD Information Technology Security Certification and Accreditation Process, 30 December 1997
(h) DoD Memo, Interim Department of Defense Information Assurance Certification and Accreditation Process Guidance, 6 July 2006
(i) SECNAV M-5510.36 DON Information Security Program Regulation, 30 June 2006
(j) COMNAVNETWARCOM 211934Z JUN 05 (NTD) 07-05, Electronic Spillage of Classified information

1. In compliance with requirements set forth in reference (a), as authorized by reference (b) (paragraph 5.9-5.9.5) and functions outlined in references (c) and (d), paragraph 2.e (22) and 3 and per references (e) through (j), you are hereby appointed as the Information Assurance (IA) (Manager/Officer) or (IAM/IAO) for (Command Name). As such, you are responsible for serving as the primary IA advisor, reporting to and advising the Local IA Authority, on all IA issues for all Operational General Service systems and networks within (Command Name).

2. As the (IAM/IAO), you are required to comply with the security requirements of reference (e), (DOD 5200.2R Chapter 2 C2.1) and hold a U.S. Government security clearance

commensurate with the level of information processed by the information system(s) for which you are responsible.

3. Your duties as the (IAM/IAO) include, but are not limited to:

a. Satisfying all responsibilities of an Authorized User as outlined in reference (b)(paragraph 5.12).

b. Developing and maintaining a (Command Name), IA program that identifies IA architecture, IA requirements, IA objectives and policies; IA personnel; and IA processes and procedures.

c. Providing security oversight for (Command Name) and subordinate commands (if applicable). This includes coordinating security measures including analysis, periodic testing, evaluation, verification, accreditation and review of information system installations at the appropriate classification level.

d. Ensuring that information ownership responsibilities are established for each (Command Name) information system, to include accountability, access approvals and special handling requirements.

e. IAM ONLY: Ensuring that IA Officers (IAOs) are appointed in writing, to include their assigned duties and responsibilities identified in reference (d) (Appendix A paragraph 4). All IAOs are also required to receive the necessary technical and IA training and policies and procedures required to carry out their respective duties.

f. Ensure compliance within the command for all IA related instructions.

g. Coordinate security measures including periodic testing, evaluation, verification and review of information system installation at the appropriate classification level within the command or organizational network structure.

h. Developing reporting procedures and ensuring that security violations and incidents are properly reported to the Computer Network Defense Service Provider, Navy Cyber Defense Operations Command and the Department of Defense reporting chain, as required. This also includes monitoring the implementation

of security guidance and coordinating and directing actions appropriate to remedy security deficiencies and following procedures set forth in accordance with references (d) and (j).

i. Ensuring that users and system support personnel have the required security clearances, authorization and need-to-know and are indoctrinated on Commander, Navy Reserve Forces Command security practices before granting access to information systems.

j. Attending periodic (IAM/IAO)-level information assurance security training as required.

k. Ensuring that system users are provided annual information assurance awareness training and that system administrator, management and network security personnel are provided appropriate systems security training for their duties.

4. This appointment is effective until rescinded in writing.

COMMANDING OFFICER

Copy to:
COMNAVRESFORCOM IAM
RCC IAM