DEPARTMENT OF THE NAVY
OFFICE OF THE SECRETARY
1000 NAVY PENTAGON
WASHINGTON DC 20350-1000

SECNAVINST 1543.2
DON CIO
30 November 2012

SECNAV INSTRUCTION 1543.2

From: Secretary of the Navy

Subj: CYBERSPACE/INFORMATION TECHNOLOGY WORKFORCE CONTINUOUS LEARNING

Ref: See Enclosure (1)

Encl: (1) References
(2) Responsibilities
(3) Definitions

1. Purpose

a. To establish policy and procedures for Department of the Navy (DON) Cyberspace/Information Technology (IT) Workforce (WF) professional development through a Continuous Learning Program (CLP) under references (a) through (q). The DON Cyberspace/IT CLP is structured to support the continuing professional development of the Cyberspace/IT WF throughout their careers. The CLP will include education, training, certification and other activities that support the sustainment and continued improvement of the capabilities of the DON Cyberspace/IT WF.

2. Scope

a. This instruction applies to Navy and Marine Corps officers and enlisted personnel (active and reserve forces) and civilians (to include non-appropriated fund (NAF) civilians), who are members of the core Cyberspace/IT WF as defined in enclosure (2).

b. This instruction also applies to personnel designated as a part of the Cybersecurity/Information Assurance (IA) workforce and requiring IA commercial certifications in accordance with references (h) through (l).

3. Policy

a. The Department of Defense (DoD) recognized cyberspace as a warfighting domain on par with air, space, land, and sea per references (f) and (g). Capability development of the DON’s workforce to establish, control, and leverage the cyberspace domain is essential to our national security. DON cyberspace policy was enumerated in reference (m). References (i) and (j) provide direction to improve the information assurance (now cybersecurity) workforce and implement continuous learning.

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

c. Professional or career development and continuous learning should be accomplished through a blended solution of formal classroom training, experience, and electronic media. Learning activities may range from on the job training to operational exercises to accredited education in accordance with references (j) through (p).

d. All civilian and military Cyberspace/IT WF personnel will participate in the CLP commensurate with their occupation, rank/grade, and position. CLP requirements are as follows:

(1) Cyberspace/IT WF members shall participate annually in 40 hours of continuous learning activities; however, if circumstances preclude 40 hours in a single year, an individual may participate in 80 hours within a two year period to satisfy the requirement. Additionally, hours completed in a previous year may be used to meet the following year’s requirement if approved by the person’s supervisor. Hours may not be carried over further than the next consecutive year.

(2) General Cyberspace/IT CLP activities may include, but are not limited to, training in multiple cyberspace specialties, leadership training, program management, joint warfighting tactics, ethics, acquisition, and rotational and developmental assignments. The DON Cyberspace/IT CL Steering

Group will identify and approve general Cyberspace/IT CLP materials and sources. Additionally, commands may identify and submit continuous learning activities through their chain of command to the Steering Group for review and approval.

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

(4) The annual continuous learning period start date is the beginning of the calendar year. If the continuous learning requirement is part of a commercial IA certification, the start date is the date identified by the certification vendor.

e. Contractors. Unless expressly provided for in the contract with the government, all responsibility for training that is required for the contractor to maintain a specific expertise, commercial certification, or continuous learning is the sole responsibility of the contractor employee and or the contractor’s employer.

4. Responsibilities See Enclosure (2)

5. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed in accordance with reference (q).

TERRY A. HALVORSEN
Department of the Navy
Chief Information Officer

Distribution:
Electronic only, via Department of the Navy Issuances Web site
http://doni.daps.dla.mil/

References

(a) 10 U.S.C. §5013
(b) OMB Circular A-130, Management of Federal Information Resources
(c) Clinger-Cohen Act, (40 USC 11315)
(d) Federal Information Security Management Act of 2002 (FISMA) (44 U.S.C. 3544)
(e) 5 U.S.C. §2301
(f) National Military Strategy for Cyberspace Operations
(g) DoD Strategy for Operating in Cyberspace, July 2011
(h) DoD Directive 8570.01 of 15 August 2004
(i) DoD 8570.01-M, Information Assurance Workforce Program of 19 December 2005
(j) SECNAVINST 5239.20
(k) SECNAV M-5239.2, Department of the Navy Information Assurance Workforce Management Manual
(l) SECNAVINST 5239.3B
(m) SECNAVINST 3052.2
(n) DON Cyber/IT Workforce Strategic Plan 2010 - 2013
(o) DoD Instruction 1400.25, Volume 250 of 18 November 2008
(p) SECNAVINST 12410.25
(q) SECNAV M-5210.1, Department of the Navy Records Management

Responsibilities

1. The Department of the Navy Chief Information Officer (DON CIO) shall:

a. Promulgate and revise uniform guidance for Cyberspace/IT WF continuous learning.

b. Lead and coordinate Cyberspace/IT WF strategic planning, ensuring that continuous learning is included in all plans.

c. Identify measures for the evaluation of Cyberspace/IT WF continuous learning.

d. Chair the DON Cyberspace/IT Continuous Learning Steering Group.

e. Ensure consistency and alignment of DON continuous learning and workforce strategic planning with DoD requirements under reference (n) and DON policies within reference (o).

2. The Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN (M&RA)) shall:

a. Provide advice on total workforce matters, policy and guidance impacting continuous learning.

b. Designate a representative to serve on the DON Cyberspace/IT Continuous Learning Steering Group.

3. The Deputy Assistant Secretary of the Navy (Civilian Human Resources (DASN(CHR)) shall:

a. Provide advice, recommendations and assistance in applying this directive to the civilian appropriated fund workforce consistent with references (n) and (o).

b. Act for ASN(M&RA) in executing assigned responsibilities under this directive for the civilian appropriated fund workforce.

4. The Chief of Naval Operations and the Commandant of the Marine Corps shall:

a. Develop and implement the Cyberspace/IT WF CLP within the Navy and Marine Corps.

b. Identify the Cyberspace/IT WF positions and personnel that are required to participate in the Cyberspace/IT WF CLP.

c. Designate a representative to serve on the DON Cyberspace/IT WF Continuous Learning Steering Group.

d. Evaluate CLP effectiveness and compliance through assessments and formal inspector general inspections.

e. Review and recommend changes to CLP guidance and programs including approved CLP training and education opportunities.

5. Commanders, Commanding Officers and Supervisors shall:

a. Ensure an annual Individual Development Plan (IDP) is developed for Cyberspace/IT WF personnel and includes continuous learning to meet the standards of the CLP.

b. Review and approve employee CLP credit submissions.

c. Monitor employee certification sustainment CLP credit submissions and status.

6. Cyberspace/IT WF Personnel shall:

a. Identify CLP requirements and CLP opportunities to participate in, and obtain supervisor approval for participation.

b. Submit CLP completion credits to the supervisor to support both DON CLP and commercial certification sustainment entities.

7. DON Cyberspace/IT Workforce Continuous Learning Steering Group shall:

a. Review CLP guidance and recommend revisions as necessary.

b. Assess Cyberspace/IT education and training programs and opportunities available from public and private sector entities. Determine those that can be used to meet continuous learning requirements, and ensure that the Cyberspace/IT WF is aware of all approved continuous learning opportunities.

c. Identify, review and approve continuous learning required to support certification sustainment, with input from the DoD CIO, the Navy the Marine Corps, and optionally, with input from commercial certification providers.

d. Review CL activities submitted by commands for CL credit approval.

e. Monitor the CLP and measure effectiveness (e.g., certification maintenance and employee participation.

Definitions

1. Career Fields include one or more occupations that require similar functional competencies.

2. Competencies are a measurable pattern of knowledge, skills, abilities, behaviors, and other characteristics that an individual needs to perform work roles or occupational functions successfully.

3. Cyberspace/IT Workforce. Military and government civilians who plan, budget, manipulate, control and archive information throughout its life cycle; develop, acquire, implement, evaluate, maintain and retire information, information systems and IT; develop the necessary policies and procedures; and apply measures that protect and defend information and information systems.

Note – Personnel assigned to Cybersecurity/IA positions as defined in references (h) through (k) are considered members of the Cyberspace/IT WF for the purposes of this instruction.

For the purposes of this instruction the Cyberspace/IT WF includes only those personnel in the following U.S. Navy and U.S. Marine Corps military occupations and civilian occupational series:

DON Civilians
2210 – IT Specialist
1550 – Computer Scientist
0854 – Computer Engineer
0855 – Electronics Engineer
0332 – Computer Operator
0335 – Computer Clerk and Assistant
0390 – Telecommunications Processor
0391 – Telecommunications
0392 – General Telecommunications
0394 – Communications Clerical
1410 – Librarian
1411 – Library Technician
1412 – Technical Information Services
1420 – Archivist
1421 – Archivist Technician

Navy Officer
1820 - Information Professional
1840 – Cyber Warfare Engineers
6420 - Limited Duty Officer Information Systems
7421 - Warrant Officer Information Systems Technician

Navy Enlisted
IT - Information Systems Technician
ITS - Information Systems Technician (Subsurface)

USMC Officer
0602 - Communications Officer
0603 - C4 Planner
0605 - Cyber Network Operations Officer

USMC Enlisted
0612 - Tactical Switching Operator
0613 - Construction Wireman
0619 - Telecommunications Systems Chief
0621 - Field Radio Operator
0622 - Digital Multi-channel Wideband Transmission Equipment Operator
0623 - Tropospheric Scatter Radio Multi-channel Equipment Operator
0627 - Satellite Communications Operator
0629 - Radio Chief
0648 - Strategic Spectrum Manager
0651 - Cyber Network Operator
0652 - Certification Authority Workstation Operator
0653 - Defense Message System Specialist
0656 - Tactical Network Specialist
0681 - Information Security Technician
0689 - Cyber Security Technician
0699 - Communication Chief

USMC Warrant
0610 - Telecommunications Systems Officer
0620 - Tactical Communications Planning Engineer Officer
0640 - Strategic Spectrum Planner
0650 - Cyber Network Operations Engineer

4. DON Cyberspace/IT Workforce Education, Training, and Career Development Program includes the structure, resources, policies, and procedures to enable the Cyberspace/IT WF to achieve the

competencies required to perform the duties and responsibilities as required by positions and to promote integrated cyberspace/IT workforce management.