



DEPARTMENT OF THE NAVY
CHIEF INFORMATION OFFICER
1 000 NAVY PENTAGON
WASHINGTON DC 20350-1000

8 February 2012

MEMORANDUM FOR DISTRIBUTION

Subj: GUIDANCE FOR CYBERSECURITY WORKFORCE OPERATING
SYSTEM/COMPUTING ENVIRONMENT CERTIFICATION COMPLIANCE
PROCESS

- Ref:
- (a) Federal Information Security Act (FISMA) of 2002
 - (b) DoD 8570.01-M, Information Assurance Workforce Improvement Program
 - (c) SECNAV Instruction 5239.20, DON Cybersecurity/IA Workforce Management, Oversight, and Compliance, of 17 Jun 10
 - (d) SECNAV Manual 5239.2, DON IA Workforce Management Manual, of 29 May 09
 - (e) ASD memo, Evolution of the Information Assurance Workforce Program, of 30 April 2010
 - (f) DONCIO memo, Guidance for Civilian Cybersecurity/Information Assurance Workforce Commercial Certification Compliance Process, of 28 Feb 2011
 - (g) UNSECNAV memo, DON Information Technology (IT) Cyberspace Efficiency Initiatives and Realignment, of 3 Dec 2010
 - (h) DON CIO memo, DON IT/Cyberspace Efficiency Initiatives and Realignment Tasking, of 20 Dec 2010

1. **Purpose.** This memorandum provides updated guidance for Department of the Navy (DON) Information Assurance Workforce (IAWF), hereafter called Cybersecurity Workforce (CSWF), commercial operating system (OS)/Computing Environment (CE) certification requirements established per references (a) through (f).

2. **Applicability.** This guidance is applicable to all civilians and military personnel who work in Information Assurance Technical (IAT), Computer Network Defense Service Provider (CND SP) (except CND-SP Manager), and Information Assurance Security Architect and Engineer positions who also perform IAT functions. Per references (b), (d), (e), and (f), cybersecurity (CS) personnel working in these functions must obtain OS/CE certifications for the operating system(s) and/or security related tools/devices they support, regardless of occupational series classification, rating, or designator, as they are our first line of defense to detect, prevent, isolate, and contain threats against our network.

3. **Background.** Technical training is essential in preparing the CSWF to keep up with emerging risks, threats, and vulnerabilities and to effectively meet the cybersecurity mission. During the past few years, the DON has advocated standardized commercial training and testing. In December 2010, the Under Secretary of the Navy and DON Chief Information Officer (CIO) directed efficiency reviews per references (g) and (h). During efficiency review discussions, the issue of moving to OS/CE certificates vice OS/CE commercial certifications was raised as a

Subj: GUIDANCE FOR CYBERSECURITY WORKFORCE OPERATING
SYSTEM/COMPUTING ENVIRONMENT CERTIFICATION COMPLIANCE
PROCESS

possible efficiency. After review and further discussion, it has been determined that the Services can effectively develop standardized training which culminates in a Service level exam.

4. **Action.** Effective immediately, OS/CE certification requirements will be satisfied, not only by commercial certifications, but also by certificates acquired through military schoolhouses, on-line or virtual training courses, and commercial classrooms. All other CSWF certification requirements remain in effect.

DON Deputy CIOs (Navy and Marine Corps) shall:

- a. Develop a plan and promulgate direction to ensure consistent OS/CE training standards which culminate in a Service-level test;
- b. Ensure OS/CE training is tracked and documented in individual development plans as well as the Service CSWF electronic management systems.

Command Information Officers shall work with Cybersecurity/Information Assurance Managers, Human Resource Officers, Training Officers, and Workforce Managers to implement these changes immediately, including enforcement and remediation action per references (b) through (f).

5. **Points of Contact.** Points of contact for assistance with this matter are as follows:

- a. DON CS WIP Office of Primary Responsibility: Mr. Chris Kelsall, (703) 695-1903, chris.t.kelsall@navy.mil;
- b. United States Navy CS WIP Office of Primary Responsibility: Ms. Theresa Everette, 703-695-4179, Theresa.m.everette@navy.mil; and
- c. United States Marine Corps CS WIP Office of Primary Responsibility: Captain Katherine Hall, USMC, (703) 693-3490, katherine.hall@usmc.mil.



Terry A. Halvorsen

Distribution:

CNO (DNS, N091, N093, N095, N097, N1, N2/N6, N3/5, N4, N8)
CMC (ACMC, ARI, M&RA, I, I&L, PP&O, C4, P&R)
ASN (RD&A)
ASN (M&RA)

Subj: GUIDANCE FOR CYBERSECURITY WORKFORCE OPERATING
SYSTEM/COMPUTING ENVIRONMENT CERTIFICATION COMPLIANCE
PROCESS

Distribution: (continued)

ASN (FM&C)
ASN (EI&E)
GC
DON/AA
DUSN/DCMO
DUSN (PPOI)
NAVIG
JAG
OLA
CHINFO
AUDGEN
CNR
DON CIO
OCHR
COMFLTCYBERCOM
COMUSFLTFORCOM
COMUSNAVEUR USNAVAF
COMPACFLT
USNA
COMUSNAVCENT
COMNAVRESFORCOM
COMNAVAIRSYSCOM
BUMED
NETC
COMNAVSEASYSKOM
FLDSUPPACT
COMNAVSUPSYSCOM
DIRSSP
CNIC
COMNAVLEGSVCCOM
NAVPGSCOL
COMNAVFACENGCOM
COMNAVSAFECEN
BUPERS
NAVWARCOL
COMUSNAVSO
ONI
COMNAVSPECWARCOM
COMSPAWARSYSCOM

Subj: GUIDANCE FOR CYBERSECURITY WORKFORCE OPERATING
SYSTEM/COMPUTING ENVIRONMENT CERTIFICATION COMPLIANCE
PROCESS

Distribution: (continued)

COMNAVDIST
NAVHISTHERITAGECOM
NAVY BAND
COMOPTEVFOR
PRESINSURV
COMSC
COMNAVCYBERFOR
COMNAVNETWARCOM
COMMARCORSYSCOM
COMMARFORCYBER
COMMARFOREUR
COMMARFORCOM
COMMARFORPAC
COMMARFORRES
COMMARFORSOUTH
COMMARSOC
CG MCCDC
CG MCRC
CG TECOM
MCNOSC
DRPM AAA WASHINGTON DC

Copy to:

PEO C4I
PEO Carriers
PEO Enterprise Information Systems
PEO Integrated Warfare Systems
PEO Land Systems
PEO Space Systems
PEO Ships
PEO Submarines
PEO Tactical Air Programs
PEO Air ASW, Assault & Special Mission Programs
EO Aviation Strike Weapons
PEO Joint Strike Fighter
PEO Littoral Combat Ships
DRPM Strategic Systems Programs
DRPM Advanced Amphibious Assault Vehicle
PM NMCI
PM NGEN