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

SECNAVINST 5239.20
DON CIO
17 June 2010

SECNAV INSTRUCTION 5239.20

From: Secretary of the Navy

Subj: DEPARTMENT OF THE NAVY CYBERSECURITY/INFORMATION ASSURANCE WORKFORCE MANAGEMENT, OVERSIGHT, AND COMPLIANCE

Ref: (a) DoD Directive 8570.01 of 15 Aug 2004
(b) DoD 8570.01-M, Information Assurance Workforce Improvement Program, of 19 Dec 2005
(c) SECNAV M-5239.2, Department of the Navy Information Assurance (IA) Workforce Management Manual to Support the IA Workforce Improvement Program, of 29 May 2009
(d) 44 U.S.C. 3544
(e) SECNAVINST 3052.2
(f) DoD Instruction 8500.2 of 6 Feb 2003
(g) SECNAVINST 5239.3B

Encl: (1) Definitions
(2) CS/IAWF Compliance Actions

1. Purpose. To establish policy and assign responsibilities for the administration of the Department of the Navy (DON) Cybersecurity (CS)/Information Assurance Workforce (IAWF) Management Oversight and Compliance Program consistent with references (a) through (g).

2. Background

a. Cyberspace and CS capabilities are essential to achieve warfighting and business missions across the operational force, expeditionary force, air, surface, or undersea domains. Furthermore, research and development and acquisition commands must employ CS fundamentals in the design through deployment phases of national security and business systems.

b. The associated mission areas all require knowledgeable CS/information assurance (IA) personnel to meet rapidly evolving mission areas. While other communities have their own management and training requirements, baseline CS/IAWF training,

manpower and personnel tracking, and commercial certification requirements have been directed by Federal statute and Department of Defense (DoD) regulations and must be adhered to by all personnel performing IA, computer network defense service provider (CND SP) and IA architect and engineer (IASAE) functions per references (a) through (c).

c. Per reference (c), the DON implemented processes and procedures necessary to ensure compliance with the Federal and DoD regulations. It is incumbent upon the DON to comply with these processes and procedures, thereby, standardizing and improving CS/IAWF skills to ensure mission readiness.

3. Scope. This instruction is applicable to:

a. The Offices of the Secretary of the Navy (SECNAV), the Chief of Naval Operations (CNO), the Commandant of the Marine Corps (CMC), and all DON commands, activities, installations, and combatant commands (where Navy is the executive agent).

b. CS/IAWF personnel as defined in reference (c). As employment of cyber capabilities is a warfighting mission, it takes many personnel involved in information technology (IT) infrastructure, network operations, maintenance, and IA to achieve military objectives through cyberspace. Personnel in the CS/IAWF have significant responsibilities for designing, developing, operating, or maintaining the security of DON IT infrastructures, systems, applications, and networks. The CS/IAWF also includes individuals who have responsibility for maintaining the confidentiality, integrity, and availability of the information contained in and transmitted from those systems and networks. CS/IAWF operations include, among other things, activities to operate and defend the Global Information Grid.

c. The CS/IA total force military (active and reserve), civilian (appropriated and non-appropriated fund), local nationals (direct, indirect, and third-country), and contractor personnel who are charged with IA functions as part of their CS duties.

d. Awareness training compliance of all information system (IS) users of DoD, DON, or combatant command (where Navy is the executive agent) IT systems.

4. Definitions. Provided in enclosure (1).

5. Policy

a. DON enterprise-wide oversight procedures shall be instituted in support of Federal and DoD direction to strengthen the CS/IAWF using methodologies compliant with references (b), (c), and (d).

b. Compliance must ensure the readiness and standardization (certification baseline that all CS/IAWF members will acquire, according to their assigned role) of the civilian, military, and contractor CS/IAWF.

c. The DON shall establish, institutionalize, and sustain processes for CS/IAWF management through the IAWF Management, Oversight, and Compliance Council (IAWF MOCC). The council will:

(1) Ensure CS/IAWF employees improve knowledge and skills from accession through separation;

(2) Coordinate with community managers to support civilian and military IAWF improvement;

(3) Foster CS/IA personnel career advancement;

(4) Oversee CS/IA total force manpower requirements analyses;

(5) Accomplish oversight and compliance through a structured metrics-based approach; and

(6) Track and enforce contractor compliance incident to the Department's total force planning.

6. Responsibilities

a. The Offices of the SECNAV, CNO, CMC, and combatant commands (where Navy is the executive agent) shall establish an oversight capability to ensure compliance with higher level directives and implementation of a CS/IAWF improvement program within the DON.

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

(1) Serve as the DON lead for CS/IAWF management compliance per reference (e);

(2) Perform the duties of the IT community leader with responsibility for oversight of CS/IAWF management within the Department;

(3) Serve as the lead for DON compliance with external reporting requirements of reference (b);

(4) Appoint a DON IA Workforce Improvement Program (WIP) office of primary responsibility (OPR) to develop a DON CS/IA WIP management plan per reference (b); and

(5) Chair the IAWF MOCC per reference (c).

c. The DON Deputy Chief Information Officer (Navy) and DON Deputy Chief Information Officer (Marine Corps) shall:

(1) Develop organizational constructs necessary to ensure compliance with references (a) through (g);

(2) Establish CS/IAWF management, oversight, and compliance processes within their respective Service;

(3) Appoint Service IA WIP OPRs to develop Service CS/IA WIP management plans per reference (b);

(4) Assist the DON CIO data collection effort by maintaining a CS/IAWF management tracking and reporting strategy;

(5) Implement oversight procedures to ensure core CS/IAWF training, certification, education, and management requirements are met and consistent per references (b) and (d) with DON oversight and Service direction;

(6) Provide representation on the IAWF MOCC Executive Board; and

(7) Ensure Services conduct, at minimum, IA WIP compliance visits per reference (c) on 5 percent of their commands, activities, and installations per year to verify documentation and compliance status.

d. Enterprise designated accrediting authorities (DAAs) shall ensure validation of CS/IAWF compliance per references (b) and (c).

e. The DON IA WIP OPRs shall:

(1) Serve as Service IA WIP OPR and coordinate with the other DoD component IA WIP OPR points of contact to develop enterprise resources to support CS/IAWF management requirements defined in law, executive orders, and DoD issuances; and

(2) Ensure Service assist visits or inspections are conducted to support unit level CS/IAWF management compliance.

f. DON acquisition community shall ensure program executive offices and systems commands carry out IAWF requirements per references (b), (c), and (d). Each command, as designated in reference (c), shall have a funded billet and specifically assigned person to carry out reference (b) IASAE enclave functional responsibilities.

g. Commanding officers, commanders, officers in charge, and civilian heads of activities, as outlined in references (a) through (g), shall:

(1) Comply with applicable IA policy/guidance;

(2) Develop a local IA WIP implementation plan;

(3) Ensure the local CS/IAWF is identified and documented in approved data bases;

(4) Ensure the local CS/IAWF member is certified and properly qualified;

(5) Authorize the command information officer (IO) to oversee the IA WIP;

(6) Empower the command information assurance manager (IAM) to ensure compliance; and

(7) Assign manpower, personnel, and training responsibilities to local human resources, administrative, and training officers to carry out CS/IAWF management.

h. Command IOs shall:

(1) Track and report standard and consistent CS/IAWF data to the next higher CIO authority and DAA;

(2) Be responsible for their own and their subordinate organization's IAWF professional's career path and training guidance, on-the-job training, and commercial certification;

(3) Provide oversight for the command IA WIP, and conduct assist visits or inspections to ensure unit level CS/IAWF management compliance; and

(4) Provide oversight for IA awareness and training programs.

i. IAMs (in commands where there is no command IO) shall:

(1) Work with the immediate superior in the chain of command (ISIC) and Service IA WIP OPRs to meet shared IAWF management oversight and compliance responsibilities; and

(2) Ensure Service electronic reporting mechanisms are used in order to report consistent data to the ISIC.

j. CS/IAWF personnel shall understand and comply with CS/IAWF requirements directed in references (a) through (g) by ensuring awareness of individual commercial certification requirements of position assigned and being personally responsible for individual development/training and certification compliance requirements.

k. IS users include all command government employees, contractors, local nationals, foreign or domestic guest researchers, visitors, or associates requiring access to information and or systems. IS users shall:

(1) Understand and comply with command IA policies and procedures; and

(2) Report awareness and training compliance through the appropriate tracking system.

l. The IAWF MOCC will:

(1) Provide DON-wide oversight of Federal and DoD IA WIP regulations per references (a), (c), (d), and (f);

(2) Develop and implement CS/IAWF management strategies, and ensure compliance with DON CS/IAWF policies by implementing key objectives of enclosure (2);

(3) Assist the Services by reviewing the enterprise picture of current and projected CS/IAWF manpower requirements, including civilian expeditionary workforce requirements, needed to meet the Department's overall IA mission afloat, ashore, and overseas;

(4) Validate CS/IA education, training, and certification standards for the CS/IAWF;

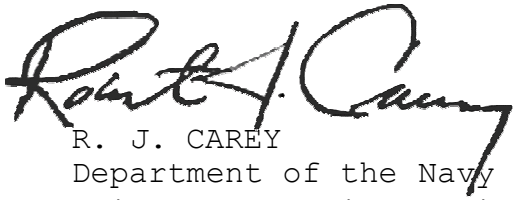
(5) Assist in career path development to ensure a standardized CS and IAWF, with a competency-based roadmap for all employees;

(6) Validate CS/IAWF competencies and competency proficiency level requirements, for both DON positions and employees, needed to meet current and future mission needs, and communicate those DON requirements to the Defense Information Assurance Program Office for inclusion in future iterations of reference (b); and

(7) Provide periodic "CS/IAWF Compliance Status" reports to the DON Information Executive Council.

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV Manual (M-)5210.1 of November 2007.

8. Reports Control. Reports contained within this instruction are exempt from report control per SECNAV M-5214.1 of December 2005.



R. J. CAREY
Department of the Navy
Chief Information Officer

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

DEFINITIONS

1. Attack Sensing and Warning (AS&W). The detection, correlation, identification, and characterization of intentional unauthorized activity, including computer intrusion or attack, across a large spectrum coupled with the notification to command and decision-makers so that an appropriate response can be developed. AS&W also includes attack/intrusion related intelligence collection tasking and dissemination; limited immediate response recommendations; and limited potential impact assessments. (DoD Directive O-8530.1 of 8 January 2001)

2. Civilian Expeditionary Workforce. A subset of the DON civilian force, who, because of their unique skill sets, are needed to meet complex DoD missions, such as stability, security, transition operations, humanitarian assistance efforts, crisis interventions, or contingency operations — can be deployed anywhere to address these operations.

3. Community Management. Encompasses processes required to shape the workforce to meet the Service mission. This includes recruiting goals, retention monitoring, re-enlistment incentives, advancement/career progression, rotation policy and transfer to fleet reserve/retirement. IAWF management encompasses officers, enlisted, and civilians that may be in either core or other functional communities.

4. Competency. Competencies are measurable knowledge, skills, abilities, behaviors or other characteristics an individual needs to perform a job or job function successfully.

5. Computer Network Defense (CND). Actions taken to protect, monitor, analyze, detect, and respond to unauthorized activity within the DoD IS and computer networks. (Joint Pub 6-0 of 30 May 1995)

6. Computer Network Defense Service Provider (CND SP). The CND SP is responsible for the implementation of CND services in a manner that effectively safeguards the network environment(s), IT infrastructure, and the confidentiality, integrity, and availability of the subscriber's information assets. Often, these protect, detect, respond, and sustain capabilities are the

responsibility of a computer emergency response team, computer incident response team, and the Network Operations Security Center. (CNDSP Standard Operating Procedure of March 2004)

7. CND Response Actions (RAs). CND RAs are deliberate, authorized defensive measures or activities that protect and defend DoD computer systems and networks under attack or targeted for attack by adversary computer systems/networks. RAs extend DoD's layered defense-indepth capabilities and increase DoD's ability to withstand adversary attacks. (CJCSI 6510.01E)

8. Cybersecurity (CS). "Prevention of damage to, protection of, and restoration of computers, electronic communications systems, electronic communications services, wire communication, and electronic communications, including information contained therein, to ensure its availability, integrity, authentication, confidentially and non-repudiation." (NSPD 54/HSPD 23 of 8 January 2008 (NOTAL))

9. Cybersecurity Workforce (CSWF). The CSWF is composed of:

a. IT Infrastructure, Operations, Maintenance and IA: Personnel who have significant responsibilities for designing, developing, operating, or maintaining the security of Federal IT infrastructures, systems, applications, and networks. This CSWF area includes individuals who have responsibility for maintaining the confidentiality, integrity, and availability of the information contained in and transmitted from those systems and networks (reference (c));

b. Domestic Law Enforcement and Counterintelligence: Personnel who analyze cyber events and environments to investigate potential threats or those individuals who participate in law enforcement, counterintelligence, and other types of investigatory activities involving IT systems, networks, and or digital evidence; and

c. Specialized CS Operations: Personnel who are engaged in highly specialized CS operations or those personnel charged with CND RAs and network AS&W. (OPM memo of November 2009, Information Request for Cybersecurity Competency Models)

10. Cyberspace. A global domain within the information environment consisting of the interdependent network of IT infrastructures, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. (DEPSECDEF Memo of 12 May 2008, The Definition of Cyberspace (NOTAL))

11. Global Information Grid. Globally interconnected, end-to-end set of information capabilities for collecting, processing, storing, disseminating, and managing information on demand to warfighters, policy makers, and support personnel.

12. Information Assurance (IA). "Measures that protect and defend information and ISs by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. These measures include providing for restoration of IS by incorporating protection, detection, and reaction capabilities." (DoD Directive 8500.01E 24 of October 2002).

13. Information Assurance Workforce (IAWF). The IAWF includes, but is not limited to, uniformed military, civilian, or contractor personnel with privileged access, system administrators, system architects, system engineers, CND service providers, certifying agents and their subordinates, red team members, blue team members, green team members, and IAMs who perform the responsibilities or functions described in references (b) and (c). These individuals are considered to have significant "security responsibilities" and must receive specialized training and be reported.

14. Network Operations. An organizational and procedural framework intended to provide DoD IS and computer network owners the means to manage their systems and networks. This framework allows IS and computer network owners to effectively execute their mission priorities, support DoD missions, and maintain the IS and computer networks. The framework integrates the mission areas of network management, information dissemination management, and IA. (Reference (b))

15. Offices of Primary Responsibility (OPRs). Staff designated to attend DoD level IA WIP meetings and who are charged with enterprise implementation of the IA WIP. There is a DON, Navy, and Marine Corps OPR.

16. Privileged Access. A person who has access to system control, monitoring, administration, criminal investigation, or compliance functions. Privileged access typically provides access to the following system controls:

a. Access to the control functions of the IS/network, administration of user accounts, etc.

b. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and key IS/network equipment/software.

c. Ability and authority to control and change program files, and other users' access to data.

d. Direct access to operating system level functions that permit system controls to be bypassed or changed.

e. Access and authority for installing, configuring, monitoring security monitoring functions of IS/networks (e.g., network/system analyzers; intrusion detection software; firewalls), or performance of cyber/network defense operations. (Reference (b))

17. Readiness. Readiness is rated proficiency level of the persons performing the work.

18. Total Force. All personnel — active and reserve military, government civilian and contractor.

CS/IAWF COMPLIANCE ACTIONS

1. The IAWF compliance actions are designed to capture key information regarding the IA WIP program implementation activity at the site level. IA compliance reviews will focus on three core areas (per the requirements identified in references (a), (b), (c), and (d)): IAWF management, IA training, and IA personnel certification. An IAWF management review/compliance visit checklist may be found in reference (c). Specific objectives of the IA compliance reviews are the following:

a. Monitor Navy and Marine Corps IA WIP implementation progress;

b. Verify command self-reported IA WIP planning documentation and initiatives;

c. Validate human resources management and control systems' collection of appropriate workforce data;

d. Confirm individual IA personnel certification and learning plans are being utilized;

e. Review IA training plans and associated training budget; and

f. Ensure Federal Information Security Act IAWF data reported is valid.

2. Compliance visits may be conducted by the following organizations/activities:

a. DoD Defense IA Program;

b. Naval Audit Service;

c. DON Headquarters level;

d. Service IA WIP OPRs;

e. Inspector General;

f. DoD Command Cyber Readiness Inspection;

g. Red Team; and

h. Blue Team assist.

3. Service OPRs are charged with ensuring commands do not receive more than one visit every 2 years, except when a reassessment is warranted.