DEPARTMENT OF THE NAVY
BUREAU OF NAVAL PERSONNEL
5720 INTEGRITY DRIVE
MILLINGTON, TN 38055-0000

BUPERSINST 5239.2
BUPERS-07
13 DEC 2010

BUPERS INSTRUCTION 5239.2

Subj: INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM TRAINING, CERTIFICATION AND WORKFORCE MANAGEMENT

Ref: (a) DoD 8570.01-M, Information Assurance Workforce Improvement Program of 19 Dec 2005
(b) SECNAV M-5239.2, Department of the Navy Information Assurance (IA) Workforce Management Manual of May 2009
(c) SECNAVINST 5239.20
(d) OPNAVINST 5239.1C

1. Purpose. To provide direction, establish guidelines, and assign responsibilities for implementing an effective Information Assurance Workforce Improvement Program (IA WIP), per references (a) through (d).

2. Background. Reference (a) establishes policy and assigns responsibilities for Department of Defense (DoD) information assurance (IA) training, certification, and workforce management. Reference (b) provides guidance and procedures for the training, certification, and management of the Department of the Navy (DON) workforce conducting IA functions in their assigned positions. Reference (c) sets the oversight and compliance policy for the DON Cybersecurity/IA Workforce Management Program. Reference (d) is the Chief of Naval Operations policy for the Navy's IA program which includes training requirements.

3. Applicability. This IA WIP plan is applicable to all Bureau of Naval Personnel (BUPERS) commands conducting IA functions to support the Department of Defense (DoD) Global Information Grid (GIG), certification and accreditation, and other Cybersecurity/ IA related tasks per references (a) through (d). It also pertains to individuals considered to be part of the core IT community, (e.g., 1600, 742x, and 642x designators or 27xx Navy Enlisted Classification (NEC)) where obtaining a commercial certification is necessary to comply with community career path training requirements.

4. Scope. References (a), (b), and (c) define the Cybersecurity/IA Workforce. All IAWF military, civilian and contractor personnel are required to meet the minimum levels of training and certification for the duties of their respective positions as defined in references (a) and (b). Once certified to the DoD baseline standard all IAWF personnel will embark on continuous learning to stay appropriately trained in technology advances.

a. Personnel assigned to IA positions are required to fulfill the certification requirements outlined in reference (a). The echelon 2 IAM will be required to certify to IAM level II and the echelon 3 command IAM will certify to IAM level I or II based upon their area of responsibility.

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

5. Action. Personnel may not perform IA duties unless they are qualified and certified to perform those duties. IAWF 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 e-Learning courses, Virtual Training Environment (VTE), command sponsored training and applicable certifications. All personnel must complete the requirements associated with their level of responsibility as determined by references (a) and (b).

a. Supervisors. Supervisors should determine how long the person has been in the DON IAWF and fulfilling tasks per reference (a) and mark at least one of the questions noted in reference (b), appendix (f). Individuals, who were in a position with "privileged access" or significant IA duties in December 2006, have until 31 December 2010 to comply with references (a) and (b). Employees newly hired and placed in a position with certification requirements have 6 months, under normal conditions, to obtain commercial certification.

b. Civilians. Per reference (b), civilian personnel managers and supervisors must ensure:

(1) The position description (PD) and the human resources hiring checklist contain the requirement to obtain commercial certification as a condition of employment;

(2) Individuals sign the updated PD to acknowledge the change of condition of employment;

(3) Appointment letters from the commanding Officer (CO) stating that a commercial certification is required per references (a) and (b);

(4) Those with "privileged access" acknowledge the IA and computing environment certification requirements;

(5) The commercial certification process is provided and direction given for the IAWF member to take a commercial certification pre-test, e-Learning, or VTE, and or classroom training;

(6) The command offers remedial training if testing is unsuccessful, up to 6 months for a new civilian hire;

(7) The supervisor mentors throughout the commercial certification process;

(8) The civilian is enrolled in a continuous learning plan documented by an individual development plan (IDP);

(9) The individual's supervisor counsels the individual as appropriate;

(10) The command offers an employee the opportunity to take the test three times;

(11) The civilian is given a letter of non-compliance and application for a waiver if warranted;

(12) The supervisor and IA professional's meetings are documented; and

(13) The employee maintains certification currency per standard procedures.

In the event the individual assigned to an IAWF position does not meet the commercial certification compliance requirements per references (a) and (b), by 31 December 2010, and all above steps have been taken, commence/continue the process to transfer the employee to a non-IAWF position or terminate employment per established Office of Civilian Human Resources guidelines.

c. Contractors. The contracting officers representative (COR) or contractor technical representative at the command validates IAWF contractor personnel compliance. CORs should ensure:

(1) All contracts contain Defense Federal Acquisition Regulation Supplement language to ensure contractors comply with reference (a);

(2) Contractor personnel meet the commercial certification requirements outlined in their contract and not be assigned nor perform any IA duties for which they are not certified; and

(3) Contractors are aware there is some "no cost" virtual training available for DoD contractors. To request an account, go to https://www.vte.cert.org/vteweb/.

d. Military. Military personnel training will be a blended solution of classroom, e-learning, exercises, and team training. supervisors should ensure:

(1) Military personnel, not trained through formal classrooms, are supported by the echelon 2 and local command; and

(2) Military personnel who do not obtain the baseline certification will not be permitted to hold the core cyber designator or NEC.

6. Responsibility

a. Echelon 2 Command Information Officer (CIO) shall:

(1) Track and report standard and consistent Cybersecurity (CS)/IAWF data to the next higher CIO authority and designated accrediting authority (DAA) per reference (c);

(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 per reference (c), conduct IA WIP compliance visits/inspections for at least 5 percent of subordinate commands to ensure unit level CS/IAWF management compliance;

(4) Provide inspection report, within 10 working days, to Navy Cyber Forces for inclusion in Navy's annual report to DoD.

(5) Provide oversight for IA awareness and training programs; and

(6) Comply with applicable IA policy/guidance.

b. Echelon 2 IAM Shall:

(1) Be responsible for the IA program for BUPERS and subordinate organizations information technology systems;

(2) Function as the focal point on behalf of, and principal advisor for, IA matters to the DAA;

(3) Establish an administrative reporting chain to ensure the appropriate information is reported to higher authority through the DAA;

(4) Support IA total force planning;

(5) Oversee an IA program that provides IA manpower and personnel tracking, IA training objectives and policies, and IA training and certification requirements;

(6) Establish procedures to ensure the command training officer sustains the IA training and certification program by reviewing and endorsing command documentation; and

(7) Provide oversight to ensure proper personnel carry out their IAWF management duties.

c. COs/Officers in Charge/Directors shall:

(1) Establish a unit level IA WIP per references (a) and (b);

(2) Ensure the command has an IA WIP that compels training managers to work with IAMs and IAWF managers to meet shared IA workforce tracking, training, certification, and reporting responsibilities;

(3) Identify all military positions and personnel required to perform IA functions described in reference (a), in the appropriate database(s) (e.g., Total Workforce Management System, Total Force Manpower Management System, or DoD component manpower or personnel systems), including foreign nationals, regardless of occupational specialty, and align them with the categories and levels described in reference (a);

(4) Per reference (a), identify all Office of Personnel Management designated GS-2210 and other IT series positions/ personnel (i.e., 0854, 1550) and enter into Defense Civilian Personnel Data System (DCPDS) the "Position Specialty Code" of INFOSEC. Enter the appropriate secondary parenthetical title or series for both primary and secondary responsibilities into DCPDS or applicable non-appropriated fund manpower system per reference (d);

(5) Promote the professional development and certification of employees who carry out IA responsibilities;

(6) Stabilize workforce rotation in the workplace so trained IA personnel are assigned to IA jobs commensurate with their certifications;

(7) Ensure all information system users (including contractors) are appropriately trained per reference (b) to fulfill their IA responsibilities before allowing them system or network access;

(8) Ensure IA contractor personnel have the appropriate appointment letter or statement of privileged access agreement, IA certification, background investigation, and are being tracked by the command COR in the appropriate data base;

(9) Ensure personnel in technical category positions maintain certifications, as required by the certifying provider, to maintain system access. IAT level I baseline and operating system certification is required prior to being authorized unsupervised privileged access to any system;

(10) Ensure personnel who are not appropriately certified within 6 months of being assigned to the IAWF position, or those who fail to maintain their certification status, not be permitted privileged access or manage information systems or IAWF personnel;

(11) Assign appropriately trained and certified personnel to IA positions;

(12) Ensure the command IAM is appointed appropriately and provided an IA designation letter (responsibilities list) and signs a statement acknowledging duties assigned the IAM position;

(13) Ensure supervisors over positions performing IA responsibilities, update all IAWF civilian position descriptions to comply with DON Chief Information Officer IA workforce guidance regarding position certification and security level requirements no later than 17 November 2010, as a condition of employment as directed by reference (c);

(14) Comply with reference (b), section 2.10. Use reference (b), appendix H to conduct an annual review of command/unit/code IA WIP programs to assess the capability, performance, and compliance against policies and requirements of references (a) through (d). Report compliance status to BUPERS CIO annually no later than 1 December;

(15) Review IA structure of the command and identify appropriate staffing requirements;

(16) Ensure CS/IAWF personnel understand and comply with CS/IAWF requirements directed in references (a), (b), and (c) by ensuring awareness of individual commercial certification requirements of position assigned and being personally responsible for individual development/training and certification compliance requirements;

(17) Ensure IAWF IDPs are created that detail specific IA training and certifications required for compliancy; and

(18) Comply with applicable IA policy/guidance.

d. Command IAM shall:

(1) Coordinate with supervisors to determine the IAWF using references (a) and (b) category descriptions;

(2) Identify, designate, document and track IA personnel training and certification against position requirements;

(3) Obtain and maintain IAM Level certification;

(4) Process and submit voucher requests to the Center for Information Dominance, U.S. Navy Credentials Program Office. Voucher request forms can be found at https://www.cool.navy.mil/costs.htm#voucher;

(5) Act as the test center coordinator;

(6) Report on DoD component training (including information assurance awareness, personally identifiable information (PII) and IAWF certification programs;

(7) Document and maintain the certification status of their IAM and IAT category personnel as long as they are assigned to those duties;

(8) Ensure each member working in an IAT environment, including developers assigned IA responsibilities, sign an Information System (IS) Privileged Access Agreement and acknowledgement of responsibilities appropriate for that IA position per reference (a), appendix 4; and

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

e. Command Training Officer shall:

(1) Ensure all training required to maintain the integrity of this instruction are planned, budgeted, and funded as directed by reference (b);

(2) Assist the IAM with the tracking of training, certification and recertification requirements per reference (b);

(3) Provide training and certification/recertification site administrators as needed; and

(4) Use service training plans to support development of the IDPs for IT professionals.

f. COR shall:

(1) Specify contractor certification and training requirements in all contracts that include acquisition of IA services;

(2) Ensure that contractor personnel, including local nationals, have the appropriate IA certification and background investigation;

(3) Ensure the capability to report in detail on individual contractor employee certification(s) and certification status. Contractor personnel must have their IA certification and function level documented per the Navy's IA WIP Manager. When feasible documentation will tracked in a Defense Manpower Data Center supported application for tracking contractors IA category or specialty, level, and certification qualification; and

(4) Enter contractor data into the required management application to support tracking contractors' IA category, specialty, level, and certification qualification.

g. IA (Total Force) Professional Shall:

(1) Commercially certify and fully qualify to perform assigned IA duties;

(2) Release their IA certification status through registration in the Defense Workforce Certification Application database at https://www.dmdc.osd.mil/appj/dwc/index.jsp; and

(3) Maintain a continuous learning plan or IDP.

h. The Authorized Information System User shall:

(1) Be responsible for the protection of data they create and comply with IA policies; and

(2) Complete and document initial annual IA awareness training and PII training.

7. Records Management. Records created as a result of this instruction, regardless of media and format, shall be managed per Secretary of the Navy Manual 5210.1 of November 2007.

D. P. QUINN
Rear Admiral, U.S. Navy
Deputy Chief of Naval Personnel

Distribution:
Electronic only, via BUPERS Web site
http://www.npc.navy.mil/

ACTION MEMO

FOR: DEPUTY CHIEF OF NAVAL PERSONNEL

FROM: Mr. Stephen Hubbard, BUPERS Command Information Officer (BUPERS-07)

SUBJECT: BUPERSINST 5239.2 (Information Assurance Workforce Improvement Program (IA WIP) Identification, Training, Certification and Workforce Management

- Approve TAB A.

- TAB A is a BUPERS instruction to establish the requirement and policy for identifying, designating, tracking, training and certification of BUPERS Information Assurance Workforce (IAWF) for personnel assigned to such positions, per DoD 8570.01M and SECNAV M-5239.2.

RECOMMENDATION: Sign TAB A.

COORDINATION: TAB B

ATTACHMENTS:
As stated

Prepared By: Mr. Steve Hubbard, BUPERS CIO, (901) 874-2302