



DEPARTMENT OF THE NAVY
BUREAU OF MEDICINE AND SURGERY
7700 ARLINGTON BOULEVARD
FALLS CHURCH, VA 22042

IN REPLY REFER TO
BUMEDINST 5239.3
BUMED-M09B15

JUL 15 2015

BUMED INSTRUCTION 5239.3

From: Chief, Bureau of Medicine and Surgery

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

Ref: (a) DoD 8570.01-M, Information Assurance Workforce
Improvement Program, January 2012
(b) SECNAV M-5239.2
(c) SECNAVINST 5239.20
(d) OPNAVINST 5239.1C
(e) Navy Telecommunication Directive 02-11
(f) BUMED memo 6000 Ser M6/09UM09B6174 of 17 Dec 09

1. Purpose. To establish guidance, provide direction, and assign responsibilities for implementing an effective Information Assurance (IA) Workforce Improvement Program (WIP), in accordance with references (a) through (f).

2. Cancellation. BUMEDINST 5239.01.

3. Scope. References (a) through (c) define the Information Assurance Workforce (IAWF). 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 Department of Defense (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).

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

4. Background. Reference (a) establishes policy and assigns responsibilities for DoD IA training, certification, and workforce management. Reference (b) provides guidance and procedures for the training, certification, and management of the DoD workforce

JUL 15 2015

conducting IA functions in assigned duty positions. Reference (c) sets the oversight and compliance policy for the Department of the Navy (DON) IAWF Management Program. Reference (d) is the Chief of Naval Operations policy for the Navy's IA program which includes training requirements.

5. Applicability. This IA WIP plan is applicable to all Bureau of Medicine and Surgery (BUMED) Headquarters personnel conducting IA functions to support the DoD Global Information Grid (GIG), certification and accreditation, and other IA related tasks per references (a) through (d). Designated IAWF personnel includes, but are not limited to, the following designators, category, and rates: Information Systems (IS) Technician, Electronics Technician, Officers, U.S. Government civilian employees, Local Nationals, and U.S. Contractors.

a. Enlisted personnel possessing the following Naval Enlisted Classification (NEC) codes are designated as IAWF personnel: 1678, 2379, 2710, 2720, 2730, 2735, 2779, 2780, 2781, and 2782. Additionally, personnel assigned to work on a system with 0000 NEC or other NEC not referenced here may also be a part of the IAWF depending on the responsibility and level of access granted.

b. Officers possessing the following designators are designated as IAWF personnel: 1600, 6180, 6420, 7180, and 7420.

c. U.S. Government and Foreign National civilian employees possessing the following designator are designated as IAWF personnel: 2210 Information Technology (Information Security) series.

d. U.S. contractors personnel are required to maintain IAWF category and level commensurate to the level of access for the system they support and/or manage as defined within this instruction.

6. 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 Information Assurance Technical (IAT) or Information System Security Manager (ISSM) will complete required Navy Skillport courses, Virtual Training Environment (VTE), command sponsored training and

JUL 15 2015

applicable certifications. All personnel must complete the requirements associated with the level of responsibility as determined by references (a) and (b).

a. Supervisors. Supervisors should use reference (b), appendix F, to determine if a person belongs to the DON IAWF and fulfilling tasks per reference (a). Per reference (e), individuals who were in a position with "privileged access" or significant IA duties in December 2006, had until 30 June 2011 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

(1) Per references (b) and (f), civilian personnel managers and supervisors must ensure:

(a) The Position Description (PD) and human resources hiring checklist contain the requirement to obtain commercial certification as a condition of employment.

(b) Individuals sign the updated PD to acknowledge the change of condition of employment.

(c) 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.

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

(e) The command offers mentors throughout the commercial certification process.

(f) The civilian is enrolled in a continuous learning place documented by an Individual Development Plan (IDP).

(g) The individual's supervisor counsels the individual as appropriate.

(h) The command offers an employee the opportunity to take the test 3 times.

JUL 15 2015

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

(j) The supervisory and IA professional's meetings are documented.

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

(2) In the event the individual assigned to an IAWF position does not meet the commercial certification compliance requirements per references (a) and (b), 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) Contractors meet the commercial certification requirements outlined in their contract and cannot be assigned nor perform any IA duties for which they are not certified.

(3) Contractors are aware there is some "no cost" virtual training available for DoD contractors. Contact the Command ISSM for virtual training resources.

d. Military. Military personnel training will be e-learning, exercises, and team training. Supervisors should ensure:

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

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

JUL 15 2015

7. Responsibility

a. Chief of Staff, Directors, Deputy Directors:

(1) Ensure the command has an IA WIP that compels training managers to work with ISSMs and IAWF managers to meet shared IAWF tracking, training, certification, and reporting responsibilities.

(2) 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 Services or DoD component manpower or personnel systems), including local nationals, regardless of occupation specialty, and align them with the categories and levels described in reference (a).

(3) Per reference (a), identify all Office of Personnel Management designed GS-2210 and other Information Technology (IT) series positions/personnel (i.e., 0335, 1550) and enter in Defense Civilian Personnel Data System (DCPDS) the "Position Specialty Code" of Information System Security Manager. 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).

(4) Promote the professional development and certification of employees who carry out IA responsibilities.

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

(6) Ensure all IS users (including contractors) are appropriately trained per reference (b) to fulfill their IA responsibilities before allowing the system or network access.

(7) Ensure ISSMs have the appropriate ISSM appointment letter and all IATs have the appropriate privileged access agreement.

(8) Ensure IA contractor personnel have the appropriate IA certification, background investigation, and are being tracked by the Command COR/Command ISSM in the appropriate database.

(9) Ensure personnel in technical category positions maintain certifications, as required by the certifying provider, to

JUL 15 2015

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 six months of being assigned to the IAWF position, or who fail to maintain their certification status, not be permitted privileged access or manage IS or IAWF personnel.

(11) Assign appropriated trained and certified personnel to IA positions.

(12) Ensure supervisors over positions performing IA responsibilities, update all IAWF civilian PD to comply with DON Chief Information Officer IAWF guidance regarding position certification and security level requirements, as a condition of employment as directed by reference (c).

(13) Comply with reference (b) section 2.10. Use reference (b) appendix H to conduct an annual review of command, unit, code IA WIPs to assess the capability, performance, and compliance against policies and requirements or references (a) through (d). Report compliance status to BUMED Chief Information Officer (CIO) annually no later than 1 December.

(14) Review IA structure of the command and identify appropriate staffing requirements.

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

(16) Ensure IAWF IDPs are created that detail specific IA training and certification required for compliancy.

(17) Comply with applicable IA policy and guidance.

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

b. Command ISSM shall:

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

JUL 15 2015

(2) Identify, designate, document, and track IA personnel training and certification against position requirements, per reference (f).

(3) Obtain and maintain appropriate ISSM 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/>.

(5) Act as the test center coordinator.

(6) Report on DoD component training (including IA awareness, Personally Identifiable Information (PII) and IAWF certification programs).

(7) Document and maintain the certification status of their ISSM 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 IS Privileged Access Agreement and acknowledge of responsibilities appropriate for IA position per references (a), appendix 4.

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

c. Command Training Officer shall:

(1) Assist the ISSM with the tracking of training, certification and recertification requirements per reference (b).

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

d. COR shall:

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

JUL 15 2015

(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 be tracked in a Defense Manpower Data Center supported application for tracking contractors IA category or specialty, level, and certification qualification.

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

e. The Authorized Information System User shall:

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

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

8. The Command ISSM is responsible for the annual review and update of this instruction.

9. Records. Records created as a result of this instruction, regardless of media and format, shall be managed per SECNAV M-5210.1 of January 2012.


A. M. DIGGS
Chief of Staff
Acting

Distribution is electronic only via the Navy Medicine Web site at:
<http://www.med.navy.mil/directives/Pages/BUMEDHQInstructions.aspx>