



DEPARTMENT OF THE NAVY

COMMANDER
NAVY CYBER FORCES
2465 GUADALCANAL ROAD, SUITE 10
VIRGINIA BEACH, VA 23459-3243

COMNAVCYBERFORINST 5239.1

N1

7 Jan 11

COMNAVCYBERFOR INSTRUCTION 5239.1

From: Commander, Navy Cyber Forces

Subj: INFORMATION ASSURANCE WORKFORCE IMPROVEMENT PROGRAM
(IA WIP)

Ref: (a) DoD Directive 8570.01 of 15 Aug 04
(b) DOD 8570.01-M, Information Assurance Workforce Improvement Program, 19 December 2005
(c) SECNAV M-5239.2, Department of the Navy Information Assurance (IA) Workforce Management Manual to Support the IA Workforce Improvement Program
(d) SECNAVINST 5239.20

Encl: (1) IA WIP Guidance
(2) IA WIP Compliance Plan and Checklist

1. Purpose. To set forth the requirements and procedures for Navy commands to professionalize and develop the Navy Information Assurance Workforce (IAWF). Enclosure (1) provides specific guidance in developing the Navy Information Assurance Workforce Improvement Program (IA WIP) and related core/targeted review areas. Enclosure (2) provides detailed instructions for conducting IA WIP site inspections. It also includes a checklist for inspections and inspection preparations. Enclosure (2) will ensure the equitable and consistent data collection across multiple organizations, and assist the Navy Cyber Forces (NAVCYBERFOR) IA WIP manager in benchmarking existing practices, reviewing implemented policy, and determining the extent of Navy IA WIP compliance.

2. Background. Information Assurance (IA), as a component of Cyber security, is a cornerstone of the Department of the Navy (DoN) transformation to a secure, interoperable, net-centric Naval Information Management/Information Technology (IT) Enterprise. The security and superiority of DoN information, information systems, and IT personnel is key to maritime dominance and national security. We take a Defense in Depth (DiD) approach to IA, layering IA principles and controls that

7 Jan 11

apply to people, processes and technology. References (a) through (d) direct services to identify IAWF billets and personnel and to develop programs to professionalize and manage their IAWF. NAVCYBERFOR is responsible to oversee and verify compliance with government IT security regulations and the Department of Defense (DoD) IA policy as it pertains to people.

3. Action. IA WIP compliance shall be monitored and reported as an element of mission readiness and as a management review item. The status of IAWF training provision and certifications shall be reported to NAVCYBERFOR as an element of mission readiness. This instruction delineates the process used by NAVCYBERFOR to determine command compliance of references (a) through (d). Echelon II Command Information Officers (CIOs) shall inspect a minimum of five percent of their subordinate commands annually to ensure IA WIP compliance. All IA WIP monitoring, oversight and compliance inspections shall be conducted using enclosure (2) of this instruction. Echelon II CIOs will forward results of all IA WIP inspections to CYBERFOR within 10 working days of the inspection outbrief. Results will be included in the Navy annual IA WIP compliance report to the DoD.

4. Report. Reporting requirements apply to all Navy commands with personnel performing IA functions, including contractors and foreign nationals.



E. D. EXNER
Chief of Staff

Distribution: Electronic only, via CYBERLINK website:
<https://www.portal.navy.mil/cyberfor/Admin/default.aspx>

7 Jan 11

IA WIP Guidance

1. The Navy IA WIP must be realized through a standardized, disciplined, and integrated approach that pulls together strategic planning, policy, and resources. Since the Information Assurance Workforce (IAWF) may reside at any shore facility, supporting establishment, operating force, undersea or afloat command, an enterprise team must be sustained to ensure continuation of the program in the coming years. Use of disparate business practices, frameworks, and methods will be minimized by implementation of enterprise processes.

2. Guiding Principles. The Navy's IAWF strategy is supported by five guiding principles. These principles shape the approach and serve as overarching guidance for implementation of DoD 8570.01-M, Information Assurance Workforce Improvement Program (IA WIP).

a. Workforce Skill Consistency. Training and certification will be standardized across the Navy to provide the necessary consistency between military, civilian, and contractor job roles and responsibilities to ensure interoperability of all segments of the IA workforce.

b. Total Force Management. IA is the responsibility of every person in the Navy with access to information systems, whether military, civilian, or contractor. Every member of the Navy team must be sufficiently trained and aware of IA practices and priorities.

c. Optimal Enterprise Solutions. Navy leadership must pursue Enterprise solutions that capitalize on lessons learned and best practices, eliminate redundancy, and ensure the best use of limited resources to achieve significant Department-wide cost efficiencies.

d. Enforcement of Laws and Regulations. It is crucial that Navy personnel protect our information technology infrastructure, and the security and privacy of information. Recent statutory and regulatory guidance to strengthen our IA posture must be adhered to throughout the organization.

7 Jan 11

e. Integration and Alignment. The complexity of this effort demands attention from organizations across the service, not limited to the functional area of information technology, but also including those who shape policy, resources, and databases for management of manpower, personnel, or training.

3. Goals

a. The Navy will develop training to support individual competencies required to perform the functions described in DoD 8570.01-M, SECNAVINST 5239.2, and the Committee for National Security Systems (CNSS) instructions 4009-4016.

b. IAWF advancement, pay, entitlement, or career milestones must be considered in individual community manpower and personnel decisions.

c. Command cultural change is required to improve the command's ability to defend the Global Information Grid. Commanding Officers must minimize moving personnel out of their IA functions and training level which would invalidate the individual's stringent training and certification requirement.

d. Standardized IAWF Mission Essential Tasks List (METL) and readiness assessments will be documented in the Defense Readiness Reporting System (DRRS) for use by the Fleet and Operating Force.

e. Future Navy manpower and personnel systems will support integrated personnel and pay processes and utilize the best IT capabilities available.

4. IA Workforce Mission. The IAWF Cyber Security mission is to provide security and mission assurance for the interdependent network of IT infrastructures, and includes the Internet, telecommunication networks, computer systems, and embedded processors and controllers in critical industries.

a. IAWF functions focus on the development, accreditation, operation, management, and enforcement of security capabilities for systems and networks.

7 Jan 11

b. Personnel performing IA functions establish IA policies and implement security measures and procedures for affiliated information systems and networks.

c. DoD 8570.01-M descriptions of the IAWF functions are summarized in the following table.

| DAA Functions | IAM Levels I, II, III | IAT Level I, II, III |
|---|--|--|
| Accredit System Authorize IA Controls Accept Risk | Oversee System Revalidate IA Controls Manage Risk | Administer System Manage IA Controls Operate (in) Risk |
| IASAE Level I, II, III | CND SP Functions | C&A Functions |
| Develop System Design IA Controls Engineer (out) Risk | Monitor System Assess IA Controls Detect Risk | Audit Certify Accredit |

Table 1. IA Functional Requirements

d. IA duties may be performed as primary or additional/embedded duties. Future Navy IAWF design will be to move away from collateral duty/embedded support to primary duty personnel who are sufficiently trained. Job tasks will be moved to the Enterprise whenever practicable, thereby standardizing the work and reducing the manpower required to accomplish the task. In some cases such as the IA Systems Architect and System Engineer (IASAE), new positions must be funded to accomplish the new functional requirement.

5. IA Workforce Structure. Commanders/Commanding Officers, in conjunction with the Designated Accrediting Authority (DAA), may title the workforce as appropriate to the job tasks they are accomplishing while fulfilling the mission as defined in the previous chapter. Some standard titles are:

a. Designated Accrediting Authority (DAA). The DAA is the official to formally assume responsibility for operating a system at an acceptable level of risk. The DAA position may not be performed by contractors. The DAA will have significant experience and normally hold the 2210 civilian series at the GS 14/15 level or equivalent. Designate the position to Information Security-I (IT-I).

7 Jan 11

DAA must complete either the DISA provided DAA Computer Base Training (CBT) or the National Defense University course granting the Committee of National Security Systems (CNSS) 4012 certificate for the following positions.

(1) Operational DAA

(2) Developmental DAA

b. IA Program Manager. The IA Program Manager (IAPM) is the person within a headquarters, acquisition, Navy Echelon II (EII), site, system, or enclave, who owns the business process and controls the funding for the system. The IAPM is accountable for the effectiveness of the program and at commands with multiple IAMs, the IAPM may be the senior Information Assurance Management (IAM). The IAPM holds a grade level comparable to the GS 13-15 level or equivalent; holds a position designated as IT-I; must be commercially certified to IAM level III and have an in-depth IT background. A contractor will not hold this position.

c. Command Information Officers. All Navy Echelon II Commands shall have a Command Information Officer (CIO) billet. Navy Echelon II CIOs report to the DDCIO (Navy) for administrative matters to their Commanding Officer for tactical matters. CIOs hold a position designated as IT-I. CIOs, normally comparable to the GS 13-15 level or equivalent should take an executive level IA education or training course. A contractor will not hold this position.

d. IA Manager. IA Manager (IAM) personnel are responsible for the implementation and operation of a DoD information system (IS) within their environment, enclave, network or individual computing system level. Incumbents ensure that IA related IS are functional and secure within the environment.

(1) Level III IAM. The IAM fulfilling the functions at the enclave level is expected to have significant IA experience and is responsible to both the local Commander and DAA for ensuring the security of an IT system or systems. The IAM positioned at the enclave, normally a GS 13-15 or equivalent is responsible for the IA program within an Echelon I or II and below or network system enclave. It is recommended that this position be filled by 2210 series with Security specialty or

7 Jan 11

officer with IA specialty or subspecialties. IAMs, at the enclave, fulfill an IT-I position and are required to train to IAM training level III. A contractor will not fulfill this position.

(2) Level II IAM. The IAM fulfilling duties at the network level, reports to the IAM at the enclave, or Information Assurance Program Manager (IAPM), except when there is a single network and then is responsible to the local Commander and service enterprise DAA. The network level IAM position, normally filled by an employee with significant security experience, is responsible for the IA program at the network level. Network level IAM positions must meet IT-I requirements and are required to train to IAM training level II. A contractor will not full fill this position except on a temporary basis with waiver. There may be more than one IAM if the command hosts more than one network.

(3) Level I IAM. The IAM fulfilling the functions at the computing level, reports to the Network IAM within a command, site, system, or enclave. Some IAMs are responsible for the IA program within a command that does not own or host a system or network. The IAM is responsible to the local Commander and DAA. In a shore command under the NMCI/NGEN structure (without another network) the IAM may be primarily engaged in training oversight and IS user compliance. If the command manpower/personnel structure is less than 25 employees, the functions of this job may be carried out by a higher level authority. This is the only IAM job that may be carried out on a collateral duty basis. IAMs will be designated IT-II security position and are required to train to IAM training level I. Contractors may hold this position.

e. Information Assurance Technical. Information Assurance Technical (IAT) personnel are responsible for the maintenance, defense and operation of DoD IS within their environment, enclave, network, or individual computing system level. Incumbents ensure that IA related IS are functional and secure within the environment. Individuals who have access to system control, monitoring, or administration functions (e.g., system administrator, system programmers) are said to have "privileged access" and therefore, require training and certification to IAT levels I, II, or III depending on the functions they perform. They must also be trained and certified on the operating

7 Jan 11

systems/environment for IS that they are required to maintain. They must hold a U.S. government security clearance and local access approvals commensurate with the level of information process on the system, network, or enclave. A person with privileged access must have a National Agency Check (NAC) and an initiated SSBI. A contractor may hold this billet. Not all inclusive, but some examples of jobs that conduct IA functions:

(1) Help Desk Customer Support/Supervisor. To carry out responsibilities of customer support, the Help Desk personnel are part of the IA workforce. Designation as IAT level I, II, or III is required depending on the tier of responsibilities. Contractors may hold this job.

(2) Help Desk Service Provider. System administrators may hold the position of the help desk service provider. Training for IAT level I-III is required for help desk tiers I, II, and III. Agency check is required. Contractors may hold this job.

(3) Data Manager. This involves planning, development, implementation, and administration of systems for storage and retrieval of data. Training to IAT level I-III is required for the data manager. Agency check is required. Contractors may hold this job.

(4) Network Administrator. This term may be used interchangeably with System Administrator, but works in the network environment. NAs normally meet the training and certification requirements for IAT level II, or to the functions specified in DoD 8570.01-M. NAs must NAC/background check.

(5) IA Officers (IAOs)

(a) IAOs are responsible to an IAM for ensuring the appropriate operational IA posture is maintained for command, organization, site, or system. If supporting an EII or enclave, the IAO will hold positions that meet IT-I requirements and hold the 2210 civilian series comparable to a GS 9-14 or equivalent position; training and certifying to the appropriate IAM/IAT level I-III. They implement and enforce system-level IA controls per program and policy guidance. A contractor will not hold this position at the Level III environment.

7 Jan 11

(b) There are other positions and titles of personnel who are involved in IA functions and responsibilities that are not listed above. Many personnel have privileged access, but will carry other titles. Anyone with privileged access and conducting IA tasks as defined in DoD 8570.01-M is a part of the IAWF and most likely an IAT.

f. Certification & Accreditation (C&A). C&A personnel perform tasks required to analyze, assess, and document IA capabilities and services of DoD information systems to establish compliance with IA requirements, identify vulnerabilities, and quantify risk. Command incumbents provide higher-level authorities such as DAAs and Certification Authority Representative (CARs) with the information needed to make or recommend an accreditation decision. These tasks are normally associated with an established IA C&A process, but may also be performed as part of other related processes or functions. At the enclave level, a Certification Authority will support CIO, Senior IAO (SIAO), DAA, CAR, IAM, or other personnel responsible for the IA oversight of an IS in the execution of their C&A-related duties. C&A personnel may do IAM or IAT functions when acting as members of a C&A team and must be trained and certified for the function for which they are performing.

(1) Certification Authority Representative (CAR). Acts as the accreditation representative on the local level and approves all C&A packages that go to the DAA. The CAR will have significant experience and normally hold the 2210 civilian series, Security specialty, normally at the GS 9-13 or equivalent level. CARs must complete the DAA training.

(2) Certification Authority (CA). The CA is the official responsible for performing the comprehensive evaluation of the technical and non-technical security features and safeguards of an IT system, application, or network. The CA, a government employee, will hold positions that meet IT-I requirements and hold the 2210 civilian series comparable to a GS 12-14 position; training and certifying will be to IAM level III. A contractor will not hold this position.

(3) Certification Agent. This individual is responsible for overseeing the site accreditation package process. Certification Agent train to the highest IAT or IAM level that

7 Jan 11

maps to their job functions and meet IT-I requirements. Contractors may hold this position.

(4) Validator. This individual is responsible for assisting in preparation of the site accreditation package. Validators train to the highest IAT or IAM level that maps to their job functions. Contractors may hold this position.

g. Computer Network Defense-Service Provider (CND-SP) Specialty. Personnel assigned as accredited CND-SPs will normally occupy a position corresponding to a single CND-SP specialty. CND-SP specialty personnel must be fully trained and certified prior to deployment to a combat environment. FLTCYBERCOM may approve a waiver for exceptions. CND-SP specialty personnel also must have the appropriate baseline IAT or IAM Certification. The following are specialty positions:

(1) CND Analyst (CND-A). CND-A personnel use data collected from a variety of CND tools to analyze events. IAT-I or II Certification, CND Certification, and Operating System Certification are required. Contractors may hold this job.

(2) CND Infrastructure Support (CND-IS). CND-IS personnel test, implement, deploy, maintain, and administer the infrastructure systems that manage the CND-SP network. IAT-I or II Certification, CND Certification, and Operating System Certification are required. Contractors may hold this job.

(3) CND Incident Responder (CND-IR). CND-IR personnel investigate and analyze activities related to cyber incidents within the NE or Enclave. IAT-I, II, or III Certification, CND Certification, and Operating System Certification are required. Contractors may hold this job.

(4) CND Auditor (CND-AU). CND-AU personnel assess systems and networks within the NE or enclave and identify deviations from acceptable configurations or policy. IAT-I, II, or III Certification, CND Certification, and OS Certification are required. Contractors may not hold this job except with waiver.

(5) CND-SP Manager (CND-SPM). CND-SPM personnel oversee the CND-SP operations. IAM-I or II Certification and CND

7 Jan 11

Certification are required. Contractors may not hold this job except with waiver.

(6) IA System Architect and System Engineer (IASAE) Specialty. Navy IASAE functions are focused primarily at the Echelon-II level to support system acquisition and development. Some job functions may occur in Echelon III commands when acting as the Research, Development Test & Evaluation (RDT&E) IA Architecture, or Lead Security Engineer representative for the Echelon-II AQ/Development office. Contractors may perform IASAE functions appropriate to their certification level, but may not be able to perform all IASAE functions. IASAE functions relating to requirements generation and entry of requirements into Statements of Work will normally require government personnel or direct government supervision.

(1) IASAE Level I. IASAE level I personnel design, develop, implement, and/or integrate a DoD IA architecture, system, or system component within their CE. Personnel must train and certify to reference (b) Chapter 10 requirements.

(2) IASAE Level II. IASAE level II personnel design, develop, implement, and/or integrate a DoD IA architecture, system, or system component within the NE. Incumbents ensure that IA-Related IS are secure within the NE. Personnel must train and certify to reference (b) Chapter 10 requirements.

(3) IASAE Level III. IASAE level III personnel design, develop, implement, and/or integrate a DoD IA architecture, system, or system component for use within CE, NE, and enclave environments. Personnel must train and certify to reference (b) Chapter 10 requirements.

(4) Users. Individuals or system processes authorized to access an information system. Users are responsible for the protection of data they create and compliance with IA policy requirements. In order to retain IT system access, users are required to complete and document that they have taken the initial and annual IA awareness training.

5. IA Civilian Community Management. The Assistant Secretary of the Navy for Manpower and Reserve Affairs (ASN M&RA) provides Enterprise policy for civilian personnel. Chief of Naval Operations (N11) supports the Navy civilian communities of

interest and teams with DoN (CIO) to foster IA civilian community health and welfare. Personnel who perform IA management-related duties would typically be identified as security, project management, or policy and planning in their parenthetical specialty title. Personnel who perform IA-technical related duties can be identified in any of the following parenthetical specialty titles: applications software, systems administration, operating systems, data management, network services, Internet, systems analysis, or customer support. Guidance for writing Civilian Position Descriptions for 2210 Series may be found on the DON CIO website.

a. IAWF Commercial Certification for Civilian Personnel

(1) Civilian personnel managers and supervisors must ensure:

(a) The position description (PD) and the Human Resources (HR) hiring checklist contain the requirement to commercially certify as a condition of employment;

(b) The Commanding Officer's appointment letter states that a commercial certification is required to meet reference (b) requirements. See appendix (c);

(c) Those with "privileged access" should acknowledge the commercial certification requirement;

(d) The commercial certification process is provided and direction given for the IA professional to take a commercial certification pre-test, e-Learning, or Virtual Training Environment (VTE), and/or classroom training;

(e) The command offers remedial training if testing is unsuccessful;

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

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

(h) The command supervisor counsels the IA professional;

7 Jan 11

(i) The supervisor/IA professional meetings are documented; and

(j) Employee maintains his certification currency per standard procedure.

(2) In the event that the IA professional does not meet the 6-month commercial certification compliance window, and all of the above steps have been taken, the command will transfer the employee to a job not requiring commercial certification.

b. Foreign Nationals/Local Nationals

(1) Foreign Nationals (FN)/Local Nationals (LNs) are not normally part of the DoN IA workforce and their employment should be minimized. FN/LN personnel are not allowed to be IAOs or IAMs. LNs can, however, be privileged users, e.g., system administrators, only with a direct supervisor who is a U.S. citizen. They can receive IAT level I training as part of their system administrator duties, but they will not hold the billet or fill the function as a member of the IA staff.

(2) LNs and FNs must comply with background investigation requirements and cannot be assigned to IAT Level III positions. "LNs or FNs may be conditionally assigned to IAM Level II. They must comply with background investigation requirements."

c. Navy Officer and Enlisted IA Community Management

(1) By delegation from CNO (N2/6), CYBERFOR is the community sponsor for the Navy military cyber communities. As the Cyber Type Commander, CYBERFOR provides oversight to IAWF with special focus on education and training.

(2) Most Navy IAWF officer and enlisted personnel will fall into IA Management levels I and II and IA Technical levels I and II. A much fewer number of personnel will fall into IAM or IAT level III or CND-SP. It is not anticipated that officers will carry out functions for IASAE. Most C&A functions will be carried out by civilians or contractors.

(3) Workforce management is required of all communities to include those where IA is carried out as an embedded duty.

7 Jan 11

Other supporting commands that will provide manpower, personnel, or training expertise are:

(a) Naval Education and Training Command (to include Intelligence, aviation, submarine, combat systems, supply Centers of Excellence)

(b) Navy Personnel Command

(c) Naval Manpower Analysis Command

(d) Centers of Excellence (Information Dominance, Combat Systems, Submarine, Aviation)

(e) Navy Reserve Forces Command

d. Navy Preferred Certification List

(1) IAT Certifications

(a) Level 1 - A+ or Network+ (In some cases both will be required)

(b) Level 2 - Security+

(c) Level 3 - GSEC or CISSP

Note - Operating system certification will be determined by environment in which individual is working.

(2) IAM Certifications

(a) Level 1 - Security+

(b) Level 2 - GSLC or CISSP

(c) Level 3 - GSLC or CISSP

(3) CND-SP Certifications. DoD 8570.01-M implementation strategy for CND-SP positions still in staffing at time of writing this publication due to impending change to CND-SP chapter of reference (b) which will include Blue and Red team responsibilities.

7 Jan 11

(4) IASAE Certifications

- (a) Level 1 - Security+
- (b) Level 2 - GSLC or CISSP
- (c) Level 3 - GSLC or CISSP

6. IA Workforce education and training categories. Warfighting effectiveness is realized by developing professionals who are highly skilled and optimally employed for mission success. Key to an enhanced and empowered workforce is training standardization.

a. The DoN has directed use of enterprise standards and solutions to implement IAWF training where ever practicable. Enterprise training solutions align the IA training available to the military, civilian, and contractor IA/CND workforce; improve the information available for decision-making and eliminate redundant expenses. Successful implementation of the IA Training standards depends on the following:

(1) Connectivity to the centralized training environment or CBT availability at deployed sites where required by the training delivery method;

(2) Coordination within the services to ensure readiness for training, proper timing of training events in relation to deployment and access to training audiences and subject matter experts (SME);

(3) Tasks that are performed in normal operations will not differ from those that are performed during wartime or under emergency deployment. Command deployment-specific operations may require a quick refresher prior to a rapid deployment; otherwise the IA common body of knowledge will function the same in war and emergency deployment as it does during normal operations;

(4) Mission-specific training established and maintained to support the proficiency necessary to support afloat and operating forces. Participation in afloat exercises focuses on standard IA practices. Security Assessment Simulations will be incorporated into operational exercises; and

7 Jan 11

(5) Personnel Qualification Standard (PQS), mentorship, on the job training (OJT), virtual training, and e-learning courses are enablers to commercial certification. The services host numerous e-learning courses. The foundations trained in these activities support IA professionals in their commercial certification, but also add consistency, standardization, and discipline to mission accomplishment.

b. IA Training Standards

(1) The Committee for National Security Standards (CNSS) was established to set standards for National Security Systems. The CNSS Education, Training, and Awareness IPT over sees the development of Committee on National Security Standards Instructions (CNSSI).

(2) IA personnel follow a training progression that supports continual skill development through individual proficiency and team proficiency. No one can expect to be fully qualified, proficient, or knowledgeable until they experience a variety of real life situations. Therefore, a system must be developed to ensure IA professionals can grow and continue to meet the cyber security mission.

(3) CNSS establishes training standards for the IAWF. These standards, along with mission and system specific training requirements such as the Computer Network Defense Operating System Environment (CND OSE), define IA training. Navy will implement an IA Training Path with baseline skill requirements conforming to CNSSI. Classroom curricula development may use the following CNSS Instructions:

(a) CNSSI 4011 Information Systems Security
Professional

(b) CNSSI 4012 Senior Security Manager

(c) CNSSI 4013 System Administrator (SA)

(d) CNSSI 4014 Information Systems Security
Officer/Manager

(e) CNSSI 4015 System Certifier

7 Jan 11

(f) CNSSI 4016 IA Risk Analyst

(4) It is intended that these specific topics be addressed over the continuum of training so that as a person grows in his/her career path he will be exposed to the applicable range of CNSSI training. Additionally, training to prepare Navy IAWF personnel for attainment of preferred certifications will be included in all pipeline training events.

c. Authorized User Awareness Training Requirements.

(1) IT users need to maintain a degree of understanding about IA policies and doctrine commensurate with their responsibilities. The focus must be on aspects of IA that impact the authorized user and place particular emphasis on actions the authorized user can take to mitigate threats and vulnerabilities to DoD ISs. Authorized users must understand that they are a critical link in their organization's overall IA posture.

(2) DISA's DoD IA Awareness CBT is the Navy baseline standard. It meets all DoD level requirements for end-user awareness training. DISA will ensure it provides distributive awareness content to address evolving requirements promulgated by Congress, Office of Management and Budget (OMB), or the Office of the Secretary of Defense. Defense Information Systems Agency (DISA's) training products can be accessed via the DoD IA Portal.

(3) DoN commands are expected to address organization specific topics and local incident reporting procedures.

d. General User Training Requirements

(1) All individuals with access to DoD IT systems are required to receive initial IA orientation before being granted access to the system(s) and annual IA awareness training to retain access. All users will be informed of their information and IS security responsibilities, and consent to monitoring.

(2) At a minimum, the following themes must be conveyed in IA initial orientation and annual awareness programs:

(a) Critical reliance on information and IS resources.

7 Jan 11

(b) Threats, vulnerabilities, and related risks associated with IS.

(c) Consequences for inadequate protection of an organization's IS resources.

(d) The essential role of the DoD employee in a successful IA program.

(3) Commands must maintain the status of user orientation and awareness compliance. Required versus actual IA orientation and awareness will be a management review item.

7 Jan 11

IA WIP Compliance Plan and Checklist

1. Introduction

a. The Navy Information Assurance Workforce Improvement Program (IA WIP) Compliance program is undertaken as part of Navy Cyber Forces (CYBERFOR) responsibility to oversee and verify component compliance with government Information Technology (IT) security regulations and Department of Defense (DoD) Information Assurance (IA) policy as it pertains to people. It consists of two levels of review:

(1) A documentation review of materials submitted by commands in response to DoD and Federal Information Security Management Act (FISMA) requirements.

(2) An on-site review at selected organizations/site locations to verify documentation and compliance status.

b. Findings from the two reviews will allow CYBERFOR to make a determination of command compliance per DoDD 8570.1 Information Assurance Workforce Training, Certification, and Management, DoD 8570.01-M Information Assurance Workforce Improvement Program (IA WIP), SECNAVINST 5239.2, SECNAVINST 5239.4, and FISMA personnel training and awareness reporting.

c. This planning document defines roles and responsibilities of participants and defines core and targeted review areas. Procedures outlined in the document are intended to promote equitable and consistent data collection across multiple organizations. It will assist CYBERFOR to benchmark existing practices, review implemented policy, and determine the extent of IA WIP compliance. The IA Site Review activities are summarized according to workflow in appendix A. This document will be used in conjunction with appendix B.

2. Objectives. This program is designed to capture key information regarding the IA WIP program implementation activity at the site level. This includes training, certification and management of IAWF personnel. Specific objectives of the IA Site Reviews are the following:

a. Monitor IA WIP implementation progress.

7 Jan 11

- c. Review Human Resources management and control systems.
- d. Confirm that IA personnel certification and learning programs are in place.
- e. Review training plans for IA and associated training budget.
- f. Confirm basis for FISMA reporting.

3. Scope. The IA Site Reviews will focus on three core areas including *IA Workforce Management*, *IA Training* and *IA Personnel Certification* per the requirements identified in DoDD 8570.01 and DoD 8570.01-M. Specific Targeted areas for review are listed in the following table:

| Target Areas for IA Site Reviews |
|---|
| Site DoD 8570.01-M Implementation Plan |
| IA Workforce Management Site Plan |
| IA Table of Organization (Manpower/Positions) |
| IA Workforce Identification Records (to include names of IA personnel; relevant data) |
| Site IA Personnel Certification Requirements |
| IA Training Plan |
| Accuracy of Manpower and Personnel Database Information |
| Privileged Access Personnel Records (relevant data) |
| Budget/Funding: Current FY |
| Budget Plan/Funding: 5-Year Defense Plan |

Table 1, Targeted Areas of IA Site Reviews

7 Jan 11

4. Pre-Site Review Activities and Coordination Procedures.
CYBERFOR is responsible for conducting the following activities prior to the IA Site Review.

a. Notifications and Arrangements

(1) CYBERFOR IA WIP Manager will coordinate with command Echelon II Information Assurance Manager (IAM) and Command Information Officer for IA Site Review - Initial contact with the review site will be made by the CYBERFOR IA WIP manager through the Echelon II IAM Point of Contact (POC). The purpose of this coordination is to:

- (a) Schedule the review.
- (b) Explain the intent and objectives of the site review.
- (c) Identify the primary site POC.
- (d) Identify site-specific core and targeted review areas.
- (e) Identify offices and ensure availability of personnel to be visited during the site review.
- (f) Ensure the availability of/access to relevant documentation and records on site.

b. CYBERFOR IA WIP Manager Confirm and Schedule IA Site Review - A final confirmation letter will be sent via email to the primary site POC and any other key personnel, if applicable, one month prior to the scheduled site review. The email will cover the following:

- (1) Request documentation for review
- (2) Request supporting documents to be readily available during site review
- (3) Confirm that appropriate personnel will be available during the site review,
- (4) Confirm meeting time, location and other logistical requirements

b. Document Review. As part of the IA Site Review, pertinent documents and records, provided by the primary site POC, will be thoroughly reviewed by CYBERFOR IA WIP Site Review Team prior to the on-site review. Documents to be reviewed include:

- (1) Component and Site IA Workforce Management Policy and Plans
- (2) IA Workforce Manpower and Personnel Information
- (3) Table of Organization/Organizational Structure
- (4) Associated Personnel Roster and qualifications
- (5) IA Training Program Plan
- (6) Continued Learning Plan
- (7) Personnel Certification Requirements Documentation
- (8) IA Technical Personnel Appointing Letters
- (9) IA Technical on the Job Practical Evaluations
- (10) IA Technical Local Operating System Certification

c. Site Review Activities and Procedures

(1) Entrance Briefing. The CYBERFOR IA WIP site review team will meet with the site primary POC and any other key personnel upon arrival. This meeting will be an opportunity for introductions and a formal explanation of the IA Site Review. This will include a review of the steps that will be taken to complete these objectives. The CYBERFOR IA WIP Site Review Team Leader will explain that team members are available to answer questions the site representatives may have and review the overall expectations of both parties. Finally, a brief overview of the post-site review actions will be provided to include documentation and outbrief reporting methods. The entrance meeting will be documented using appendix C.

(2) Site Review. As supported by the IA Site Review objectives, the CYBERFOR IA WIP Site Review Team will be reviewing, interviewing and observing various areas of the site's IA Workforce Management, Training and Personnel Certification program and plans.

7 Jan 11

The review is an assessment of the site's IA organization according to the requirements identified in DoD 8570.01-M. To ensure data integrity and metrics validity, appendix B has been created. The composition of this checklist corresponds to the Core Review Targets for the IA Site Reviews, as stated in Table 1. Refer to appendix B.

(3) Exit Briefing. The CYBERFOR IA WIP Site Review Team Leader will facilitate an exit meeting at the conclusion of the visit. The team will provide a brief summary of identified effective and "best practices" as well as challenge areas or issues. Each challenge area or issue will be discussed along with preliminary corrective actions necessary to achieve required DoD 8570.01-M compliance. The site's primary POC and other key personnel will have the opportunity to address these challenge areas/issues and will be urged to work collaboratively with their Echelon II IAM and the CYBERFOR IA WIP Manager's office to determine a suitable plan of action to solve the issues. The exit meeting will be documented using appendix D.

d. Post-Site Review Activities/Site Review Reporting. The CYBERFOR IA WIP Site Review Team will prepare an outbrief based on the findings and outcomes of the IA Site Review. The report will highlight identified "best-practices" for information sharing purposes (with permission) as well as challenge areas/issues that require greater attention and management support. Recommendations, a proposed plan of action, and any next steps will also be documented to ensure progress toward DoD 8570.01-M compliance. The outbrief will be distributed to all participants of the IA Site Review as well as the appropriate chain of command. The information in the report will also be used to support Inspector General requests on IA WIP compliance matters. Upon completion of the report, reviewed site/organization leadership will have an opportunity to review/comment prior to the final publishing.

7 Jan 11

Appendix A: IA Site Review Workflow

1. E-Mail notification to the Echelon II IAM and review site.
 - a. Date/time for review.
 - b. Provide objectives.
 - c. Set up logistics.
 - d. Ensure availability of relevant documentation and records on site.
2. Follow-up phone call to initial notification.
 - a. Confirm e-mail notification with site POC.
 - b. Further discuss review procedures.
 - c. Overview of pre-site review responsibilities.
3. Final e-mail confirmation and request for documentation and list of key personnel.
 - a. Request site provide initial documentation required to prepare for site review.
 - b. Request list of site key personnel.
 - c. Confirm all logistics for site visit.
 - d. Request any questions site has about review to be forwarded via digitally signed e-mail.
4. Conduct pre-site review of site documentation.
 - a. Site IA Workforce Management policy/plans.
 - b. Command Activity Manpower Document
 - c. Command Enlisted Distribution Verification Report
 - d. IAWF Training plan.
 - e. Certification requirements documentation (e.g., Civilian Position Description, Assignment letters, etc.)

7 Jan 11

5. Entrance brief to conduct site review.
 - a. Meeting with site POC and key personnel.
 - b. Introductions and explanation of purpose and objectives.
6. Conduct site review.
 - a. Review through interviews and observation the site's IAWF management plan in the following areas:
 - (1) Policy
 - (2) Training
 - (3) Certification
7. Exit briefing to end site review.
 - a. Meeting with site POC and key personnel to discuss findings of review.
 - b. CYBERFOR will provide summary of best practices and items requiring corrective action to site and Echelon II IAM.
 - c. Site to provide Plan of Action and Milestones for items requiring corrective action within 10 working days of exit briefing.
8. Forward to CYBERFOR (N1), CIO, and ODAA site review results.
 - a. Continue following results until all corrective actions have been resolved.
 - b. Report results in annual qualitative report on IA WIP to Department of the Navy Chief Information Officer.

7 Jan 11

Appendix B: IA Site Review Checklist

Navy Information Assurance Workforce Management Implementation Checklist:

| | |
|-------------------|--|
| Critical Element | Have IA, Training and Admin/HR management personnel at the site level developed and implemented IA Workforce Improvement Program (IA WIP)? |
| Purpose | To assess the capability, performance and compliance against the policies and requirements of DoDD 8570.1 and DoD 8570.01-M. |
| Core Review Areas | IA Workforce Management, IA Training, IA Certification |
| Method | Review of IA WIP program plans, including documentation and procedures review. |

YES NO N/A Source Comment

A. IA Workforce Management

| | YES | NO | N/A | Source | Comment |
|---|-----|----|-----|-----------------------------------|---------|
| 1. Is the CO familiar with DoD 8570.01-M IA WIP and FISMA requirements? | | | | Lead IAM | |
| 2. Have the DoD 8570.01-M and DoN IA WIP Plans been distributed to the IA workforce? | | | | Commanding Officer, N/G6, IAWF | |
| 3. Has the site developed and implemented its own IA WIP instruction/guidance? | | | | Site IAM; Personnel Officer | |
| 4. Are all IA positions with IA functions identified by category and level in the site's Activity manpower Document? (DoD 8570.01-M, Chapter 7, paragraph C7.2.2) | | | | DCPDS; TWMS; FLTMS | |
| 5. Are the DON CIO, CNO N6, and CYBERFOR official messages on the IA Workforce Management accessible? | | | | Admin; official web sites | |
| 6. Number of IA Positions identified by category/level in the personnel and staffing database(s) (DoD 8570.01-M, Chapter 8, paragraph 8.2.7.1.2) | | | | DCPDS; TWMS; IAWF Management Tool | |
| 7. Number of IA positions filled by category and level in the personnel and staffing database(s) (DoD 8570.01-M, Chapter 8, paragraph 8.2.7.1.5) | | | | DCPDS; TWMS; IAWF Management Tool | |

7 Jan 11

| | | | | | |
|--|--|--|--|---|--|
| 8. Are all positions and personnel with IA responsibilities identified in the appropriate database, regardless of occupational specialty? | | | | DCPDS; TWMS; IAWF Management Tool | |
| 9. Are these individuals further identified as performing IA responsibilities as primary or as an additional, or embedded duty? <i>(DoD 8570.01-M, Chapter 8, paragraphs C8.2.7.1.3 and C8.2.7.1.4)</i> | | | | DCPDS; TWMS;IAWF Management Tool | |
| 10. Have all civilian IAWF position descriptions been updated to include certification to be held as a condition of employment? | | | | Local Official Files | |
| 11. For NSPS personnel do individual performance goals include certification attainment/maintenance requirements? | | | | | |
| 12. Have all IA personnel with privileged access completed a "Privileged Access Agreement?" Show examples. | | | | Local Official Files; TWMS | |
| 13. Do all IA personnel with privileged access have a Common Access Card to control access? | | | | IAWF Members | |
| 14. Number of users who completed the IA orientation/awareness annual training requirement versus total number of authorized users <i>(DoD 8570.01-M, Chapter 8, paragraph C8.2.7.4)</i> | | | | Electronic training jacket; FLTMS | |

B. IA Training

| | | | | | |
|---|--|--|--|--------------------------------|--|
| 1. Does the site have an official IA Training Plan and is it implemented? | | | | Official Site Training Plan | |
| 2. Does the training plan state specialized training necessary (i.e. HBSS for privileged access users performing IA functions)? | | | | Official Site Training Plan | |

7 Jan 11

| | | | | | |
|--|--|--|--|--|--|
| 3. How many of those with privileged access responsibilities have received the required training. | | | | Training Records; IAWF Management Tool | |
| 4. What is the timeline for training the remaining individuals identified with significant security responsibilities to receive specialized training? | | | | Local IA Training or Implementation Plan | |
| 5. What are the reasons for all identified personnel not having yet received specialized training (i.e., insufficient funding, insufficient time, courses unavailable, personnel are not registered)? | | | | Commanding Officer; Site IAM and IAWF Members | |
| 6. Are detailed training records maintained for all IA personnel? (records that indicate the exact training for each member) | | | | Local Training Records | |
| 7. Does the site have on the job training or job qualification requirements for assigned IAWF personnel? | | | | Local IA WIP Implementation Plan | |
| 8. Is an oversight structure in place that manages the IA training program? Is there documentation of IA training oversight structure to include Training Officers and supervisors of IAM, personnel with privileged access, CND, IASAE, C&A and all IA professionals? | | | | Commanding Officer; Local IA WIP Implementation Plan/Training Plan | |
| 9. Percentage of personnel with privileged access who have documented completion of the OJT/JQR requirement. | | | | Local Official Records; Training Officer | |
| 10. Are plans for continued learning a part of the training plan? | | | | IA WIP Plan Electronic support | |
| 11. Percentage of personnel with privileged access, IAMs, CND, IASAE, C&A and DAA completing continuing training requirements. | | | | Training Database; Local Training Records; IAWF | |

7 Jan 11

| | | | | | |
|---|--|--|--|---|--|
| 12. Have all assigned DAAs completed the DoD DAA training within 60 days of assignment (or the NDU/IRMC CNSSI No. 4012 course/certificate) or equivalent training? (DoD 8570.01-M, Chapter 5, paragraphs C5.3.1.1 and C5.3.2) | | | | Local Training Records; Training Database | |
| 13. Do IAWF personnel have individual training plans. | | | | Local Official Records | |

C. IA Certification Program

| | | | | | |
|---|--|--|--|---|--|
| 1. Does the site have a plan that establishes timelines and procedures for all current and new IA personnel to be appropriately certified for their primary position? | | | | Commanding Officer; Training Officer; Local IA WIP Implementation Plan | |
| 2. What is the oversight process in place that ensures all site contracts include that contractors must hold the appropriate certification? (DFARS 48 CFR Parts 239 and 252 RIN 0750-AF 52 DFARS: Information Assurance Contractor Training and Certification (DFARS Case 2006-D023)) | | | | Commanding Officers; Acquisition and Budget Personnel; Electronic Databases; IAWF Members | |
| 3. Has the site identified appropriate "operating system certification" requirements and trained their workforce with privileged access? | | | | Commanding officers; Supervisors | |
| 4. Is an oversight process in place that ensures all incumbents and new hires are trained, certified and recertified? | | | | Commanding Officer; IAWF Members | |

7 Jan 11

Appendix C: Entrance Meeting Notes Template

Agenda

Introduction

Overview of site review objectives and activities

Meet with site operational leadership representative(s) to determine the level of support they receive for IA operations

Question and Answer/Meeting wrap-up

Meeting Date:

Meeting Location:

| Name | Phone Number | Email |
|------|--------------|-------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

7 Jan 11

Appendix D: Exit Meeting Notes Template

Agenda

- Highlight identified areas of best practice
- Review areas needing improvement
- Provided recommended actions for improvement
- Question and Answer/Meeting wrap-up

Meeting Date:

Meeting
Location:

| Attendee Name | Phone Number | Email |
|---------------|--------------|-------|
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |
| | | |

7 Jan 11

Concerns and Issues

Review
Area

Comments/Concerns/Recommendation

| | |
|--|--|
| | |
| | |
| | |
| | |
| | |

Best Practices

Record any potential best practices found during the review.

| |
|--|
| |
| |
| |
| |