DoD 8570.01-M

Information Assurance Workforce Improvement Program

December 19, 2005
Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer

ASSISTANT SECRETARY OF DEFENSE
6000 DEFENSE PENTAGON
WASHINGTON, DC 20301-6000

NETWORKS AND INFORMATION INTEGRATION

December 19, 2005

FOREWORD

This Manual is issued under the authority of DoD Directive 8570.1 "Information Assurance Training, Certification, and Workforce Management," August 15, 2004 (Reference (a)). It provides guidance and procedures for the training, certification, and management of the DoD workforce conducting Information Assurance functions in assigned duty positions. It also provides information and guidance on reporting metrics and the implementation schedule for Reference (a).

This Manual applies to the Office of the Secretary of Defense, the Military Departments, the Chairman of the Joint Chiefs of Staff, the Combatant Commands, the Office of the Inspector General of the Department of Defense, the Defense Agencies, the DoD Field Activities, and all other organizational entities in the Department of Defense (hereafter referred to collectively as the "DoD Components").

This Manual is effective immediately and is mandatory for use by all the DoD Components.

Send recommended changes to the Manual to the following address:

Director
Information Assurance Directorate Assistant Secretary of Defense for Network and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/ DoD CIO)
1155 Defense Pentagon
Washington, DC 20301-1155

The DoD Components may obtain copies of this Manual through their own publications channels. Other Federal agencies and members of the public may obtain copies of this Manual from the U.S. Department of Commerce, National Technical Information Service, 5285 Port Royal Road, Springfield, VA 33261. An electronic version of this Manual can be viewed and downloaded from the following web site: http://www.dtic.mil/whs/directives.

John G. Grimes
Assistant Secretary of Defense for
Networks and Information Integration/
DoD Chief Information Officer

TABLE OF CONTENTS

FIGURES

TABLES

REFERENCES

(a) DoD Directive 8570.1, “Information Assurance Training, Certification, and Workforce Management,” August 15, 2004
(b) DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
(c) DoD Directive 8500.1, “Information Assurance (IA),” October 24, 2002
(d) DoD Directive O-8530.1, "Computer Network Defense (CND)," January 8, 2001
(e) DoD 5200.2-R, “Personnel Security Program,” January 1987
(f) DoD Instruction 5200.40, “ DoD Information Technology Security Certification and Accreditation Process (DITSCAP),” December 30, 1997
(g) Section 2224 of Title 10, US Code, “Defense Information Assurance Program”
(h) Section 278g-3 of Title 15, US Code, (as added by the Computer Security Act of 1987)
(i) Office of Management and Budget Circular A-130, “Management of Federal Information Resources, Transmittal 4,” November 30, 2000, Appendix 3
(j) DoD Directive 1000.25, “DoD Personnel Identity Protection (PIP) Program,” July 19, 2004
(k) DoD Instruction 7730.64, “Automated Extracts of Manpower and Unit Organizational Element Files,” December 11, 2004
(l) DoD Instruction 1336.5, “Automated Extracts of Active Duty Military Personnel Records,” May 2, 2001
(m) DoD Instruction 7730.54, “Reserve Components Common Personnel Data System (RCCPDS),” August 6, 2004
(n) DoD Instruction 1444.2, “Consolidation of Automated Civilian Personnel Records,” September 16, 1987
(o) Office of Personnel Management Job Family Position Classification Standard for Administrative Work in the Information Technology Group, GS-2200; Information Technology Management, GS-2210, May 2001, revised August 2003
(p) Section 3544 of Title 44, US Code (as added by the Federal Information Security Management Act (FISMA) of 2002)
(q) DoD 8910.1-M, “Procedures for Management of Information Requirements”, June 30, 1988
(r) Committee on National Security Systems Instruction No. 4009, “ National Information Security System Glossary,” revised May 2003
(s) Chapter 51 of Title 5 US Code
(t) International Standards Organization/International Electronics Commission (ISO/IEC) 17024 “General Requirements for Bodies Operating Certification of Persons” April 2003
(u) Code of Federal Regulations Title 29 , Volume 4 revised as of July 1 2004 Section 1607

ACRONYMS

Acronym	Meaning
AIS	Automated Information System
ASD(NII)/DoD CIO	Assistant Secretary of Defense for Networks and Information Integration/DoD Chief Information Officer
CBT	Computer Based Training
CE	Computing Environment
CIO	Chief Information Officer
CO/XO	Commanding Officer/Executive Officer
CMIS	Corporate Management Information System
COOP	Continuity of Operations Plan
Council	ASD(NII)/ DoD CIO and USD P&R Information Assurance Training, Certification, and Workforce Management Oversight Advisory Council
COTR	Contracting Officer's Technical Representative
DAA	Designated Approving Authority
DCPDS	Defense Civilian Personnel Data System
DEERS	Defense Eligibility Enrollment Reporting System
DIMHRS	Defense Integrated Military Human Resources System
DISA	Defense Information Systems Agency
DMDC	Defense Manpower Data Center
DoD	Department of Defense
FISMA	Federal Information Security Management Act
FN	Foreign National
GIG	Global Information Grid
IA	Information Assurance
IAM	Information Assurance Manager
IAT	Information Assurance Technical
IAVA	Information Assurance Vulnerability Alert
INFOCON	Information Operations Condition
INFOSEC	"Security" (The parenthetical title in DCPDS for civilian personnel performing security (IA) functions)

Acronym	Meaning
IASE	Information Assurance Support Environnent (DoD IA Portal)
IS	Information System
ISO/IEC	International Organization for Standardization /International Electro-technical Commission
IT	Information Technology
e-JMAPS	e-Joint Manpower and Personnel System
LN	Local National
NE	Network Environment
NIPRNet	Non-classified Internet Protocol Router Network
OMB	Office of Management and Budget
OJT	On the Job Training
OPM	Office of Personnel Management
PSC	Position Specialty Code
SIPRNet	Secret Internet Protocol Router Network
USD(P&R)	Under Secretary of Defense for Personnel and Readiness
WBT	Web-Based Training
WO	Warrant Officer

C1. CHAPTER 1

GENERAL INFORMATION

C1.1. PURPOSE

This Manual:

C1.1.1. Implements DoD Directive 8570.1 (Reference (a)).

C1.1.2. Provides guidance for the identification and categorization of positions and certification of personnel conducting Information Assurance (IA) functions within the DoD workforce supporting the DoD Global Information Grid (GIG) per DoD Instruction 8500.2 (Reference (b)). The DoD IA Workforce includes but is not limited to all individuals performing any of the IA functions described in this Manual. Additional chapters focusing on personnel performing specialized IA functions including system architecture and engineering, computer network defense, certification and accreditation, and vulnerability assessment will be published as changes to this Manual.

C1.1.3. Establishes IA workforce oversight and management reporting requirements to support Reference (a).

C1.1.4. No requirements of this Manual are intended to be inconsistent with applicable law.

C1.2. DEFINITIONS. See Appendix 1.

C1.3. DoD IA WORKFORCE MANAGEMENT OBJECTIVES:

C1.3.1. Develop a DoD IA workforce with a common understanding of the concepts, principles, and applications of IA for each category, level, and function to enhance protection and availability of DoD information, information systems, and networks.

C1.3.2. Establish baseline technical and management IA skills among personnel performing IA functions across the DoD enterprise.

C1.3.3. Provide warfighters qualified IA personnel in each category and level.

C1.3.4. Implement a formal IA workforce skill development and sustainment process, comprised of resident courses, distributive training, blended training, supervised on-the-job training, exercises, and certification/recertification.

C1.3.5. Verify IA workforce knowledge and skills through standard certification testing.

C1.3.6. Augment and expand on a continuous basis the knowledge and skills obtained through experience or formal education.

C1.4. RESPONSIBILITIES

In addition to the responsibilities listed in Reference (a) and Section 3544 of Title 44 (Reference (p)), this Manual assigns the following:

C1.4.1. The Assistant Secretary of Defense for Networks and Information Integration/Department of Defense Chief Information Officer (ASD(NII)/DoD CIO) shall:

C1.4.1.1. Coordinate changes and updates to this Manual to maintain state of the art functional and certification requirements for the IA workforce.

C1.4.1.2. Develop, coordinate, and publish baseline certification requirements for personnel performing specialized IA functions.

C1.4.1.3. Coordinate the implementation and sustainment requirements of this Manual to include supporting tools and resources (e.g., conferences, website, database integration, workforce identification).

C1.4.1.4. Establish in coordination with USD(P&R) an Information Assurance Training, Certification, and Workforce Management Oversight Advisory Council (Council) to ensure that the requirements of Reference (a) and this Manual are met. The Council shall:

C1.4.1.4.1. Meet at least annually at the call of the DoD DCIO and include, at a minimum, representatives from the Chairman of the Joint Chiefs of Staff; USD(P&R); USD for Intelligence; USD for Acquisition, Technology, and Logistics (AT&L); the Military Departments and Services; Defense Information Systems Agency (DISA); and the U.S. Strategic Command. Members must be government employees.

C.1.4.1.4.2. Establish an approval process for IA certifications to be added to or deleted from the Certification Table (AP3.T1). Certifications must have a strong correlation to the IA workforce levels and functions.

C1.4.1.4.3. Review and update the IA levels, functions, and associated certification requirements contained in this Manual.

C1.4.1.4.4. Monitor the DoD IA certification program process improvements.

C1.4.1.4.5. Conduct formal and informal reviews of Component programs and plans to validate/approve compliance with DoD baseline IA workforce management requirements. Reviews will include the following:

C.1.4.1.4.5.1. Component implementation and sustainment plans for IA workforce identification, training, certification, management, reporting, and documentation requirements as established in this Manual and References (a) and (p).

C1.4.1.4.5.2. Component plans and methodologies to track, monitor, and document completion of IA Awareness orientation and training requirements for all network users as established in this Manual and References (a) and (p).

C1.4.1.4.6. Report recommended actions to the ASD(NII) and USD(P&R) based on these reviews or other information available to it (such as FISMA Reporting Information or reports required by this Manual) to improve the program.

C1.4.1.4.7. Conduct assessments to ensure the validity of the IA workforce functions, training, and certification requirements per 29 CFR Volume 4, Section 1607 (Reference (u)).

C1.4.1.4.8. Prioritize enterprise-wide requirements for development of training content to address gaps and deficiencies

C1.4.1.5. Prepare an annual IA workforce training and certification report.

C1.4.1.6. Require the Director of the Defense Information Systems Agency (DISA) to:

C1.4.1.6.1. Provide appropriate representation to the Council.

C1.4.1.6.2. Coordinate with the DIAP, USD(AT&L), and the Components to develop and maintain an online resource correlating DoD IA training products and classes to requirements defined in law, executive order, regulation, policy, or guidelines. Additionally, provide information correlating IA functional requirements (Chapters 3, 4, and 5) to workforce categories and levels to core IA training curriculum.

C1.4.1.7. Require the Defense-wide Information Assurance Program (DIAP) to provide IA workforce management oversight and coordination for the requirements established in this Manual.

C1.4.2. The Under Secretary of Defense for Personnel and Readiness (USD(P&R)) shall support and provide appropriate representation to the Council. The Defense Activity for Non-Traditional Education Support (DANTES) will manage the certification testing process requirement for the Department.

C1.4.3. The Under Secretary of Defense for Intelligence shall provide appropriate representation to the Council to represent the Intelligence community.

C1.4.4. The Heads of the DoD Components shall:

C1.4.4.1. Comply with the responsibilities and requirements of Reference (a) and this Manual.

C1.4.4.2. Provide support for the continuous improvement of the IA workforce management processes and maintenance of requirements. Provide appropriate representation as required to the Council.

C1.4.4.3. Provide for initial IA orientation and annual awareness training to all authorized users to ensure they know, understand, and can apply the IA requirements of their system(s) in accordance with Reference (a) (see Chapter 6).

C1.4.4.4. Per Reference (a), identify all positions performing information system management or privileged access IA functions by category and level as described in Chapters 3, 4, and 5 of this Manual. This applies to all positions with IA duties, whether performed as primary or additional/embedded duties (see Chapters 2-5 and 7). This requirement applies to military and civilian positions including those staffed by local nationals (LN), and to contractors if made part of the contract.

C1.4.4.5. Identify all IA function requirements to be performed by contractors in their statement of work/contract.

C1.4.4.6. Train, certify, and obtain the proper security clearance for all personnel identified as part of the IA workforce to accomplish their IA duties (see Chapters 3-5 and Appendices 2 and 3).

C1.4.4.6.1. Include requirements for IA training on all DoD Components and local policy and procedures as part of the IA program.

C1.4.4.6.2. Ensure IA personnel performing IA functions obtain/maintain a certification corresponding to the highest level function(s) required by their position.

C1.4.4.6.3. Nominate, as appropriate, other certifications that correspond to the IA functions established for a particular level. Nominations may include operating system certifications that include the appropriate IA requirements. Provide nominations to the Council.

C1.4.4.6.4. Obtain the appropriate security clearance per Reference (b) prior to granting unsupervised privileged access or management responsibilities to any DoD system.

C1.4.4.7. Identify, track, and monitor IA personnel performing IA functions (as described in Chapters 3, 4, and 5) to ensure that IA positions are staffed with trained and certified personnel (see Chapter 7).

C1.4.4.8. Collect metrics and submit reports to the ASD(NII)/DoD CIO to support planning and analysis of the IA workforce and annual FISMA reporting per Reference (p) (see Chapter 8).

C1.4.4.9. Establish, resource, and implement plans, policies, and processes to meet the requirements of Reference (a) and this Manual (see Chapter 9).

C1.4.4.10. Identify all GS-2210 positions/personnel using the Office of Personnel Management specified parenthetical titles per OPM Job Classification Standard (Reference (o)). Enter the appropriate parenthetical title for both primary and/or additional duty responsibilities in

DCPDS or equivalent civilian personnel database. This is required for all DoD personnel even if the individual performs more than two 2210 specialties.

C1.4.4.11. Enter "INFOSEC" as the "Position Specialty Code" into DCPDS per Reference (a) for all positions/personnel performing IA functions described in Chapters 3, 4, and 5 as primary, additional, or embedded duty and their category and level.

C1.4.4.12. Ensure that all DoD contracts requiring performance of IA functions (specified in Chapters 3 and 4) include the requirement to report contractor personnel's IA certification status and compliance with this Manual. Contractors also must meet the security clearance requirements of Reference (b).

C1.4.4.13. Ensure personnel performing IA functions on national security systems meet the Committee on National Security Systems training requirements. This is in addition to the requirements of this Manual.

C1.4.4.14. Include appropriate IA content in officer accession programs; Flag, Commanding/Executive Officer (CO/XO), and Warrant Officer (WO) indoctrination; and Component professional military education. The training is intended to develop leadership understanding of the critical importance of information assurance to the successful execution of DoD's mission at all levels of the Department of Defense.

C2. CHAPTER 2

IA WORKFORCE STRUCTURE OVERVIEW

C2.1. INTRODUCTION

C2.1.1. IA functions focus on the development, operation, management, and enforcement of security capabilities for systems and networks. Personnel performing IA functions establish IA policies and implement security measures and procedures for the Department of Defense and affiliated information systems and networks.

C2.1.2. IA measures protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation. This includes providing for their restoration by incorporating protection, detection, and reaction capabilities.

C2.1.3. IA duties may be performed as primary or additional/embedded duties, by a DoD employee (civilian, including LNs, or military) or by a support contractor(including LNs).

C2.1.4. As a condition of privileged access to any information system, PERSONNEL PERFORMING IA FUNCTIONS described in this Manual must satisfy both preparatory and sustaining DoD IA training and certification requirements (see Chapters 3-5). Additionally, personnel with Privileged Access must complete a "Privileged Access Agreement", a sample of which is shown in Appendix 4, Components may expand the requirements of this agreement to meet their needs.

C2.1.5. The certification requirements of this Manual apply to DoD civilian employees, military personnel, local nationals, and support contractors performing the IA functions below and described in detail in Chapters 3-5.

C2.1.6. Personnel performing IA duties addressed by this policy include the following IA oversight responsibilities:

C2.1.6.1. Work closely with data owners, information system owners, and users to ensure secure use and operation of IS and networks.

C2.1.6.2. Ensure rigorous application of IA policies, principles, and practices in the delivery of all information technology (IT) services.

C2.1.6.3. Maintain system audit functions and periodically review audit information for detection of system abuses.

C2.1.6.4. Identify IA requirements as part of the IT acquisition development process.

C2.1.6.5. Assess and implement identified corrections (e.g., system patches and fixes) associated with technical vulnerabilities as part of the Information Assurance Vulnerability Management program, consistent with References (a) and (b), DoD Directive 8500.1 (Reference (c)), and DoD Directive O-8530.1 (Reference (d)).

C2.1.6.6. Maintain configuration control of hardware, systems, and application software.

C2.1.6.7. Identify and properly react to security anomalies or integrity loopholes such as system weaknesses or vulnerabilities.

C2.1.6.8. Install and administer user identification or authentication mechanisms.

C2.1.7. The IA workforce training and certification program establishes a baseline of validated (tested) knowledge that is relevant, recognized, and accepted across the Department of Defense.

C2.2. IA WORKFORCE CATEGORIES AND LEVELS

C2.2.1. This Manual identifies two overall categories within the IA workforce: Technical and Management. These categories are subdivided into three levels each based on functional skill requirements and system environment focus (see Chapters 3, 4, and 5).

C2.2.2. The levels and functional requirements in both the technical and the management categories apply to civilian, military, and contractor personnel (including those LNs specifically authorized to perform IA functions per Reference (b).

C2.2.3. The levels and functions provide the basis to determine all IA technical and management staffing requirements. They also provide a framework for the identification of IA technical and management positions and qualified personnel (or those who can become qualified) across the Department of Defense.

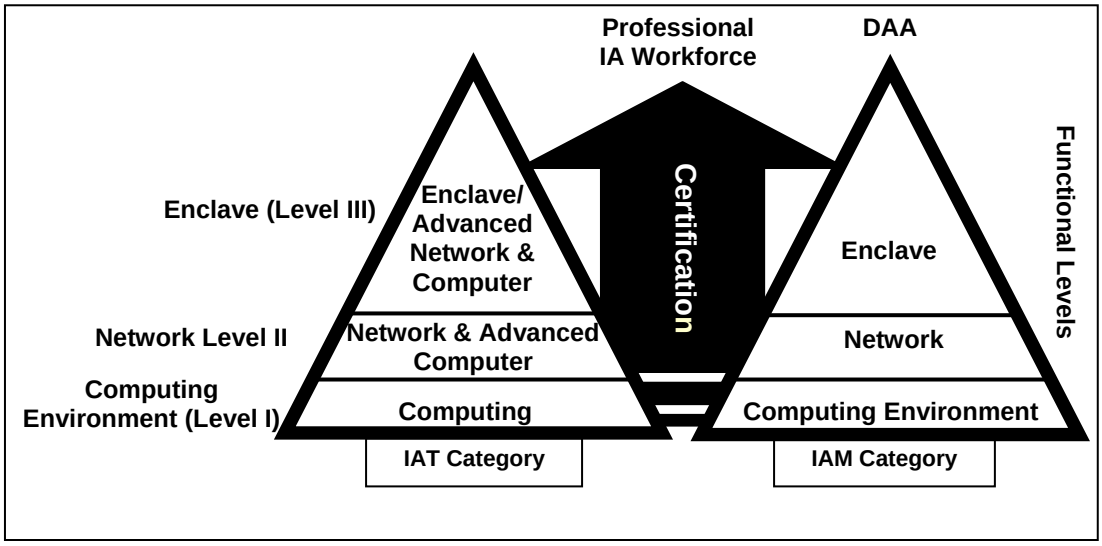
C2.2.4. Each DoD position responsible for IA functional requirement(s) must be correlated with a category and level. Assigning position levels based on functions across the Department of Defense establishes a common framework for identifying the IA workforce.

C2.2.5. A position may include functional requirements spanning multiple levels. In these cases, the level, and related certification requirements will be those of the highest level functions. Individuals performing both IAT and IAM category functions must hold certifications appropriate to the functions performed in each category.

C2.2.6. IA workforce categories and levels do not necessarily correlate to civilian grades, military ranks, or any specific occupational classification standard.

C2.2.7. Figure C2.F1., below, provides an overview of the IA workforce structure.

Figure C2.F1. Overview of IA Workforce Structure



C2.3. TRAINING AND CERTIFICATION PROGRAMS

C2.3.1. IA certification programs are intended to produce IA personnel with the demonstrated ability to perform the functions of their assigned position. Each category and skill level has specific training and certification requirements. Meeting these requirements will require a combination of formal training, experiential activities such as on-the-job training, and continuing education. These training and certification requirements must be provided by the Department of Defense at no cost to government employees (military or civilian).

C2.3.2. The DoD Components must use certifications approved (and published as part of this Manual) by the office of the ASD(NII)/DoD CIO as the minimum certification requirement.

C2.3.3. Approved certifications will demonstrate close correlation to the IA categories, levels, and functions described in Chapters 3-5 and demonstrate portability throughout the Department of Defense, Federal government, and private sector.

C2.3.4. Individuals in IA positions, as defined in Chapters 3-5, not meeting certification requirements must be reassigned to other duties, consistent with applicable law. Those individuals in IA positions not meeting certification requirements may perform those duties under the direct supervision of an appropriately certified individual until certification is attained unless waived due to severe operational or personnel constraints (see paragraphs C3.2.4.2., C3.2.4.3., C.4.2.3.2.1., or C4.2.3.4.2.).

C2.3.5. Appendix 2 establishes the IA workforce certification requirement and criteria for assigned responsibilities. It also includes a requirement for the periodic review of DoD categories, functions, levels, and the approval of their associated certifications.

C2.3.6. Appendix 3 provides a matrix of certifications and the categories/levels to which they apply. IA workforce members must obtain the certification corresponding to their IA functions as defined in Chapters 3, 4, and 5 and Appendix 3.

C2.3.7. Certification holders must ensure that their certificates stay active. Expired certifications must be renewed. Expired certifications are not to be considered in the workforce reports.

C2.3.8. To support IA professionals the DoD IA Portal (formerly known as the IA Support Environment (IASE)) provides DoD IA policy, training requirements, and DoD-sponsored training. The IA Portal is located at http://iase.disa.mil/.

C2.3.9. Contractor personnel supporting IA functions in Chapters 3 and 4 shall be appropriately certified prior to being engaged. The contracting officer will ensure that contracting personnel are appropriately certified and provide verification to the Defense Eligibility Enrollment System (DEERS). Additional training on local or system procedures may be provided by the DoD organization receiving services.

C2.3.10. Organizations employing LNs should coordinate in advance with appropriate offices such as the Status of Forces Agreement, the Local or Country Human Resources section of OPM, local unions, and/or training. Effective coordination will greatly enhance the capability to achieve the requirements of this Manual.

C2.3.11. Personnel IA certification status and renewal rates are management review items per Reference (b).

C3. CHAPTER 3

IA WORKFORCE TECHNICAL CATEGORY

C3.1. INTRODUCTION

C3.1.1. This chapter provides detailed position guidelines and IA functions for each level within the Technical category.

C3.1.2. The functions associated with each of these levels are intended to be baseline DoD requirements. The DoD Components are expected to have additional requirements reflecting their operating policy and information system technical environment. The requirements of this Manual do not exempt individuals from meeting their own organization's standards and requirements.

C3.2. TECHNICAL CATEGORY DESCRIPTION

C3.2.1. This category comprises IA Technical (IAT) Levels I, II, and III.

C3.2.2. Personnel required to perform any technical category IA functions (one or more functions) at any level must be certified to the highest level function(s) performed. An IAT position's functional requirement(s) for a particular level establish the basis for the individual's certification requirement.

C3.2.2.1. The IAT category's functional requirements are cumulative. Thus, an IAT Level II or III position requires mastery of the functional requirements of the preceding levels.

C3.2.3. IAT Category Training Requirements:

C3.2.3.1. Participation in initial training (classroom, distributive, or blended) before, or immediately on, assignment of IA responsibilities. Training need not result in award of a military specialty code (e.g., Military Occupational Specialty, Navy Enlisted Classification Code, and/or Air Force Specialty Code), but must be sufficient to meet minimum certification standards outlined here and in Appendices 2 and 3.

C3.2.3.2. Completion of an on-the-job skills practical evaluation to meet functional requirements listed in this chapter.

C3.2.3.3. Completion of sustainment training/continuing education as required to maintain certification status. For planning purposes the standard is normally a minimum of 20 to 40 hours annually, or 120 hours over three years.

C3.2.4. IAT Category Certification Requirements:

C3.2.4.1. The certification program for IAT category positions must include the functions identified for that level. All IAT category personnel, whether they perform IA functions as primary or additional/embedded duty, must be certified based on the IA functions of the position.

C3.2.4.1.1. Within six months of assignment of IA duties, all IAT personnel must achieve the appropriate IA certification unless a waiver is granted per paragraphs C3.2.4.2 or C3.2.4.3. below.

C3.2.4.1.1.1. Individuals performing IA functions and who are DoD employees or contractors on the effective date of this Manual have up to four years to comply with the certification requirements, based on Component plans to meet the implementation milestones established in Chapter 9.

C3.2.4.1.1.2. New hires' qualification periods begin the date they start in the position (i.e., they must obtain the appropriate certification within six months of being assigned IA functions).

C3.2.4.1.2. IAT Level I certification is mandatory prior to IA Managers authorizing unsupervised privileged access for personnel performing IAT Levels I through III functions described in this Chapter.

C3.2.4.2. Designated Approving Authorities (DAAs) may waive the certification requirement under severe operational or personnel constraints. The waiver will be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint. Waivers will not extend beyond six months, must include an expiration date, and be documented in the individual IA training record. Consecutive waivers for personnel are not authorized except as noted in paragraph C3.2.4.3. Waivers must be a management review item per Reference (b). Uncertified IAT Level Is are not authorized to have unsupervised privileged access.

C3.2.4.3. IAT category personnel must be fully trained and certified prior to deployment to a combat environment. The DAA may approve a waiver for certified IAT-Is to fill level IAT-II or IAT-III billets without attaining the appropriate certification while deployed to a combat environment. The DAA may grant an interim waiver limited to the period of the deployment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed six months following date of return from combat status.

C3.2.4.4. Personnel in technical category positions must be issued and retain an appointing letter to their IA duties including a statement of responsibilities for the system. Appendix 4 provides a sample statement of acceptance of responsibilities. Components will appropriately edit this form and maintain a completed copy in the individual's personnel record or with the COTR for contractors.

C3.2.4.5. Personnel in technical category positions must maintain certifications, as required by the certifying provider, to retain privileged system access. Level 1 certification is required prior to being authorized unsupervised privileged access.

C3.2.4.6. Personnel who are not appropriately certified within six months of assignment to a position or who fail to maintain their certification status must not be permitted privileged access. The DoD Components will develop programs to address remedial training and conditions for individuals to attain or return to certified status.

C3.2.4.7. The DoD Components must document and maintain the certification status of their IAT category personnel as long as they are assigned to those duties. Identification and tracking requirements are addressed in Chapter 7.

C3.2.4.8. To support the GIG infrastructure security requirements, certification standards apply equally to DoD civilian, military, and contractor personnel including those staffed by LN (with conditional privileged access per Reference (b)).

C3.2.4.8.1. New contract language must specify certification requirements. Existing contracts must be modified, at an appropriate time during the phased implementation, to specify certification requirements

C3.2.4.8.2. Per References (b) and (d) and DoD 5200.2-R (Reference (e)), LNs and FNs must comply with background investigation requirements and cannot be assigned to IAT Level III positions.

C3.2.4.8.3. In addition to the baseline IA certification requirement for their level, IATs with privileged access MUST OBTAIN APPROPRIATE COMPUTING ENVIRONMENT (CE) CERTIFICATIONS for the operating system(s) they support as required by their employing organization. This requirement ensures they can effectively apply IA requirements to their hardware and software systems.

C3.2.4.8.4. New hire civilians and contractor personnel must agree as a “condition of employment” that they will obtain the appropriate certification for the position to be filled.

C3.2.4.8.5. All personnel must agree to release their certification qualification(s) to the Department of Defense.

C3.2.4.9. Technical category training requirements are summarized in Table C3.T1.

Table C3.T1. IAT Workforce Requirements

Civilian, Military, Contractor* (Including Civilian or Contractor LNs)	**IAT Level I - III (FN and LN Levels I & II only)**
Initial Training **	Yes
IA Certification (from approved list)	Yes (within six months)
Initial On the Job Practical Evaluation	Yes (for initial position)
Computing Environment (CE) Certification	Yes
Maintain Certification Status	Yes (as required by certification)
Continuous Education or Sustainment Training	Yes (as required by certification (e.g., ISC 2 requires 120 hours within 3 years))
Background Investigation	As required by IA level and Reference (b)
Sign Privileged Access Statement	Yes
*Contractor category, level, and certification requirements to be specified in the contract **Classroom, distributive, blended, government, or commercial provider	

C3.3. IAT LEVEL I

C3.3.1. IAT Level I personnel make the CE less vulnerable by correcting flaws and implementing IAT controls in the hardware or software installed within their operational systems. IAT Level I position requirements are listed in Table C3.T2.

Table C3.T2. IAT Level I Position Requirements

IAT Level I	
Attribute	**Level**
Experience	Normally has zero to four years of experience in IA technology or a related field.
System Environment	CE.
Knowledge	Applies basic knowledge of IA concepts, practices, and procedures within the CE.
Supervision	Works under supervision and typically reports to a CE manager.
Other	Actions are usually authorized and controlled by policies and established procedures.
IA Certification & Operating System Certification	Within six months of assignment to position and mandatory for unsupervised privileged access.

C3.3.2. Table C3.T3. lists the specific functional requirements associated with the IAT Level I position. Personnel performing these functions, regardless of their occupational title (e.g., system administrator, help desk technician, information system technician, mechanic, infantry, logistics, aviation mechanic, etc,) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C3.T1.

Table C3.T3. IAT Level I Functional Requirements

T-I.1. Recognize a potential security violation, take appropriate action to report the incident as required by regulation, and mitigate any adverse impact.
T-I.2. Apply instructions and pre-established guidelines to perform IA tasks within CE.
T-I.3. Provide end user IA support for all CE operating systems, peripherals, and applications.
T-I.4. Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to their CE.
T-I.5. Apply CE specific IA program requirements to identify areas of weakness.
T-I.6. Apply appropriate CE access controls.

T-I.7. Install and operate the IT systems in a test configuration manner that does not alter the program code or compromise security safeguards.
T-I.8. Conduct tests of IA safeguards in accordance with established test plans and procedures.
T-I.9. Implement and monitor IA safeguards for CE system(s) in accordance with implementation plans and standard operating procedures.
T-I.10. Apply established IA security procedures and safeguards and comply with responsibilities of assignment.
T-I.11. Comply with system termination procedures and incident reporting requirements related to potential CE security incidents or actual breaches.
T-I.12. Implement online warnings to inform users of access rules for CE systems.
T-I.13. Implement applicable patches including information assurance vulnerability alerts (IAVA), information assurance vulnerability bulletins, and technical advisories for the CE operating system(s).
T-I.14. Understand and implement technical vulnerability corrections.
T-I.15. Enter assets in a vulnerability management system.
T-I.16. Apply system security laws and regulations relevant to the CE being supported.
T-I.17. Implement DoD and component password policy.
T-I.18. Implement specific IA security countermeasures.
T-I.19. Obtain and maintain IA certification appropriate to position.

C3.4. IAT LEVEL II

C3.4.1. IAT Level II personnel provide network environment (NE) and advanced level CE support. They pay special attention to intrusion detection, finding and fixing unprotected vulnerabilities, and ensuring that remote access points are well secured. These positions focus on threats and vulnerabilities and improve the security of systems. IAT Level II personnel have mastery of the functional requirements of the IAT Level I position. IAT Level II position requirements are listed in Table C3.T4.

Table C3.T4. IAT Level II Position Requirements

IAT Level II	
Attribute	**Level**
Experience	Normally has three to seven years in IA technology or a related area.
System Environment	NE and advanced CE.
Knowledge	• Mastery of the functional requirements of the IAT Level I position. • Applies knowledge and experience with standard IA concepts, practices and procedures within the network environment.
Supervision	Works under general supervision and typically reports to network manager.
Other	Relies on experience and judgment to plan and accomplish goals within the NE.
IA Certification & Operating System Certification	Within six months of assignment to position.

C3.4.2. Table C3.T5. lists the specific functional requirements associated with the IAT Level II position. Personnel performing these functions, regardless of their occupational title (e.g., system administrator, help desk technician, information system technician, mechanic, infantry, logistics coordinator) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C3.T1.

Table C3.T5. IAT Level II Functional Requirements

T-II.1.	Demonstrate expertise in IAT Level I CE knowledge and skills.
T-II.2.	Examine potential security violations to determine if the NE policy has been breached, assess the impact, and preserve evidence.

T-II.3.	Support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the NE.
T-II.4.	Recommend and schedule IA related repairs in the NE.
T-II.5.	Perform IA related customer support functions including installation, configuration, troubleshooting, customer assistance, and/or training, in response to customer requirements for the NE.
T-II.6.	Provide end user support for all IA-related applications for the NE.
T-II.7.	Analyze patterns of noncompliance and take appropriate administrative or programmatic actions to minimize security risks and insider threats.
T-II.8.	Manage accounts, network rights, and access to NE systems and equipment.
T-II.9.	Analyze system performance for potential security problems.
T-II.10.	Assess the performance of IA security controls within the NE.
T-II.11.	Identify IA vulnerabilities resulting from a departure from the implementation plan or that were not apparent during testing.
T-II.12.	Provide leadership and direction to IA operations personnel.
T-II.13.	Configure, optimize, and test network servers, hubs, routers, and switches to ensure they comply with security policy, procedures, and technical requirements.
T-II.14.	Install, test, maintain, and upgrade network operating systems software and hardware to comply with IA requirements.
T-II.15.	Evaluate potential IA security risks and take appropriate corrective and recovery action.
T-II.16.	Ensure that hardware, software, data, and facility resources are archived, sanitized, or disposed of in a manner consistent with system security plans and requirements.
T-II.17.	Diagnose and resolve IA problems in response to customer reported incidents.
T-II.18.	Research, evaluate, and provide feedback on problematic IA trends and patterns in customer support requirements.
T-II.19.	Ensure IAT Level I personnel are properly trained and have met OJT program requirements.
T-II.20.	Perform system audits to assess security related factors within the NE.
T-II.21.	Develop and implement access control lists on routers, firewalls, and other network devices.
T-II.22.	Install perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc., and enhance rule sets to block sources of malicious traffic.
T-II.23.	Work with other privileged users to jointly solve IA problems.
T-II.24.	Write and maintain scripts for the NE.
T-II.25.	Demonstrate proficiency in applying security requirements to an operating system for the NE or CE used in their current position.
T-II.26.	Implement applicable patches including IAVAs, IAVBs, and TAs for their NE.

T-II.27. Adhere to IS security laws and regulations to support functional operations for the NE.
T-II.28. Implement response actions in reaction to security incidents.
T-II.29. Support the design and execution of exercise scenarios.
T-II.30. Support Security Test & Evaluations (Part of Certification and Accreditation Process).
T-II.31. Obtain and maintain IA certification appropriate to position.

C3.5. IAT LEVEL III

C3.5.1. IAT Level III personnel focus on the enclave environment and support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the CE, NE, and enclave environments. IAT Level III personnel have mastery of the functional requirements of both the IAT Level I and Level II positions. IAT Level III position requirements are listed in Table C3.T6.

Table C3.T6. IAT Level III Position Requirements

IAT Level III	
Attribute	**Level**
Experience	Normally has at least seven years in IA technology or a related area.
System Environment	Enclave Environment, advanced NE, and advanced CE.
Knowledge	• Expert in all functional requirements of both IAT Level I and IAT Level II positions. • Applies extensive knowledge of a variety of the IA field's concepts, practices, and procedures to ensure the secure integration and operation of all enclave systems.
Supervision	• Works independently to solve problems quickly and completely. • May lead and direct the work of others. • Typically reports to an enclave manager.
Other	• Relies on extensive experience and judgment to plan and accomplish goals for the enclave environment. • Supports, monitors, tests, and trouble shoots hardware and software IA problems pertaining to the enclave environment. • Must be a U.S. Citizen.
IA Certification & Operating System Certification	Within six months of assignment to position.

C3.5.2. Table C3.T7. lists the specific functional requirements associated with the IAT Level III position. Personnel performing these functions, regardless of their occupational title (e.g., system administrator, help desk technician, information system technician, aviation mechanic, infantry, logistics coordinator) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C3.T1.

Table C3.T7. IAT Level III Functional Requirements

T-III.1.	Mastery of IAT Level I and IAT Level II CE/NE knowledge and skills.
T-III.2.	Recommend and schedule IA related repairs within the enclave environment.
T-III.3.	Coordinate and ensure end user support for all enclave applications and operations.
T-III.4.	Lead teams to quickly and completely solve IA problems for the enclave environment.
T-III.5.	Formulate or provide input to the enclave's IA/IT budget.
T-III.6.	Plan and schedule the installation of new or modified hardware, operating systems, and software applications ensuring integration with IA security requirements for the enclave.
T-III.7.	Determine whether a security incident is indicative of a violation of law that requires specific legal action.
T-III.8.	Direct the implementation of appropriate operational structures and processes to ensure an effective enclave IA security program including boundary defense, incident detection and response, and key management.
T-III.9.	Provide direction to system developers regarding correction of security problems identified during testing.
T-III.10.	Evaluate functional operation and performance in light of test results and make recommendations regarding certification and accreditation.
T-III.11.	Examine enclave vulnerabilities and determine actions to mitigate them.
T-III.12.	Monitor and evaluate the effectiveness of enclave IA security procedures and safeguards.
T-III.13.	Analyze IA security incidents and patterns to determine remedial actions to correct vulnerabilities.
T-III.14.	Develop the enclave termination plan to ensure that IA security incidents are avoided during shutdown and long-term protection of archived resources is achieved.
T-III.15.	Develop and apply effective vulnerability countermeasures for the enclave.
T-III.16.	Develop and manage IA customer service performance requirements.
T-III.17.	Develop IA-related customer support policies, procedures, and standards.
T-III.18.	Write and maintain scripts required to ensure security of the enclave environment.

T-III.19. Design perimeter defense systems including intrusion detection systems, firewalls, grid sensors, etc.; enhance rule sets to block sources of malicious traffic; and establish a protective net of layered filters to prevent, detect, and eradicate viruses.
T-III.20. Schedule and perform regular and special backups on all enclave systems.
T-III.21. Establish enclave logging procedures to include important enclave events,, services and proxies,, log archiving facility.
T-III.22. Provide OJT for IAT Level I & II DoD personnel.
T-III.23. Analyze IAVAs and Information Assurance Vulnerability Bulletins for enclave impact and take or recommend appropriate action.
T-III.24. Obtain and maintain IA certification appropriate to position.

C4. CHAPTER 4

IA WORKFORCE MANAGEMENT CATEGORY

C4.1. INTRODUCTION

C4.1.1. This chapter provides detailed position guidelines and IA functions for each level within the Management category.

C4.1.2. The functions associated with each of these levels are intended to be baseline DoD requirements. The DoD Components are expected to have additional requirements reflecting their operating policy and information system technical environment. The requirements of this Manual do not exempt individuals from meeting their own organization's standards and requirements.

C4.2. MANAGEMENT CATEGORY DESCRIPTION

C4.2.1. This Category comprises IA Management (IAM) Levels I, II, and III, as well as the DAA function covered in Chapter 5.

C4.2.2. The levels and functional requirements in the management category are not necessarily cumulative. Table C4.T1. provides IAM category requirements.

Table C4.T1. IAM Workforce Requirements

Civilian, Military, or Contractor* (Including LNs)	**IAM Level I - III (FN/LN Levels I & II** only)**
Initial Training ***	Yes
IA Certification (from approved list)	Yes (within six months)
OJT Evaluation	No
CE Certification	No
Maintain Certification Status	Yes (as required by certification)
Sustainment Training	Yes (as required by certification (e.g., ISC 2 requires 120 hours within three years))
Background Investigation	As required by IA level and Reference (b)
* Requirements to be stated in contract. ** FN/LN IAM Level II must meet conditions of References (b), (d), and (e). *** Classroom, distributive, blended, or commercial provider.	

C4.2.3. IAM Category Certification Requirements:

C4.2.3.1. The certification requirement for IAM category positions includes all the functions identified for that level. All management category personnel, whether they perform IA functions as primary or as an additional/embedded duty, will be certified based on the IA functional requirements of the position.

C4.2.3.1.1. Personnel required to perform any management category IA function(s) (one or more functions) at any level must be certified to the highest level function(s) performed. An IAM position's functional requirement(s) for a particular level establish the basis for the certification requirement.

C4.2.3.1.2. IAM positions that also perform IAT functions must also obtain the appropriate technical level certification and complete the other IAT level requirements prior to being granted unsupervised privileged access.

C4.2.3.2. Within six months of assignment of IA duties, management category personnel must achieve the appropriate IA certification for their level. The requirements in paragraphs C3.2.4.1.1.1. and C3.2.4.1.1.2. for current and new hire DoD employees also apply to IAMs.

C.4.2.3.2.1. DAAs may waive the certification requirement under severe operational or personnel constraints. The waiver will be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint.

C4.2.3.2.2. Waivers will not extend beyond six months and must include an expiration date and be documented in the individual IA training record. Consecutive waivers for personnel are not authorized except as noted in paragraph C4.2.3.4.2. Waivers must be a management review item.

C4.2.3.3. Personnel in management category positions must maintain certifications, as required by the certification provider, as described in Appendix 3, to retain the position.

C4.2.3.4. Personnel not certified within six months of assignment of IA duties or who fail to maintain their certified status will not be permitted to carry out the responsibilities of the position. The DoD Components must develop programs to address remedial training and to establish conditions allowing management personnel to return to certified status.

C4.2.3.4.1. If after appropriate remediation efforts individuals do not meet certification requirements, they must be reassigned to other duties.

C4.2.3.4.2. IAM category personnel must be fully trained and certified prior to deployment to a combat environment. However, the DAA may grant an interim waiver for personnel required to fill IAM II or III level billets with IAM I or IAM II certified individuals who cannot obtain the appropriate certification WHILE deployed in a combat environment. The interim waiver may be granted by the DAA for the period of deployment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed six months following the date of return from the combat environment.

C4.2.3.5. The DoD Components must document and maintain the certification status of their management category personnel as long as they are assigned to those duties. Identification and tracking requirements are addressed in Chapter 7.

C4.2.3.6. Personnel in management category positions will retain an appointing letter assigning them IA responsibilities for their system(s) per Reference (b). If a management category position requires IA privileged access, a statement of responsibility for the system(s) will also be executed per Reference (b). Appendix 4 provides a sample statement of acceptance of responsibilities.

C4.2.3.7. In support of GIG infrastructure security requirements, certification standards apply equally to DoD civilian, military, contractor personnel, and local nationals.

C4.2.3.7.1. New contract language must specify certification requirements. Existing contracts must be modified to specify certification requirements during the phased implementation described in Chapter 9.

C4.2.3.7.2. LNs or FNs may be conditionally assigned to IAM Level II but may not be assigned to IAM Level III positions (per Reference (b)). They must comply with background investigation requirements per Reference (e).

C4.3. IAM LEVEL I

C4.3.1. IAM Level I personnel are responsible for the implementation and operation of a DoD IS or system component within their CE. Incumbents ensure that IA related IS are functional and secure within the CE. IAM Level I position requirements are listed in Table C4.T2.

Table C4.T2. IAM Level I Position Requirements

IAM Level I	
Attribute	**Level**
Experience	Usually an entry level management position with zero to five years of management experience.
System Environment	CE IAM.
Knowledge	Applies knowledge of IA policy, procedures, and structure to develop, implement, and maintain a secure CE.
Supervision	• For IA issues, typically reports to an IAM Level II (NE). • May report to other management for other CE operational requirements.
Other	Manages IA operations for a CE system(s).
IA Certification	Within six months of assignment to position.

C4.3.2. Table C4.T3. lists the specific functional requirements associated with the IAM Level I position. Personnel performing these functions, regardless of their occupational title (e.g., ISSO, IAO, ISSM, logistics manager, pilot, infantry officer) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C4.T1.

Table C4.T3. IAM Level I Functional Requirements

M-I.1. Use federal and organization specific published documents to manage operations of their CE system(s).
M-I.2. Provide system related input on IA security requirements to be included in statements of work and other appropriate procurement documents.
M-I.3. Support and administer data retention and recovery within the CE.
M-I.4. Participate in the development or modification of the computer environment IA security program plans and requirements.
M-I.5. Validate users' designation for IT Level I or II sensitive positions, per Reference (b).
M-I.6. Develop procedures to ensure system users are aware of their IA responsibilities before granting access to DoD information systems.
M-I.7. Recognize a possible security violation and take appropriate action to report the incident, as required by directives.
M-I.8. Supervise or manage protective or corrective measures when an IA incident or vulnerability is discovered.
M-I.9. Ensure that system security configuration guidelines are followed.
M-I.10. Ensure that IA requirements are integrated into the Continuity of Operations Plan (COOP) for that system or component.
M-I.11. Ensure that IA security requirements are appropriately identified in computer environment operation procedures.
M-I.12. Monitor system performance and review for compliance with IA security and privacy requirements within the computer environment.
M-I.13. Ensure that IA inspections, tests, and reviews are coordinated for the CE.
M-I.14. Participate in an IS risk assessment during the Certification and Accreditation process.
M-I.15. Collect and maintain data needed to meet system IA reporting requirements.

M-I.16. Obtain and maintain IA certification appropriate to position.

C4.4. IAM LEVEL II

C4.4.1. IAM Level II personnel are responsible for the IA program of an IS within the NE. Incumbents in these positions perform a variety of security related tasks, including the development and implementation of system information security standards and procedures. They ensure that IS are functional and secure within the NE. IAM Level II position requirements are listed in Table C4.T4.

Table C4.T4. IAM Level II Position Requirements

IAM Level II	
Attribute	**Level**
Experience	Usually has at least five years of management experience.
System Environment	NE IAM.
Knowledge	Applies knowledge of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure NE.
Supervision	• For IA issues, typically reports to an IAM Level III (Enclave) Manager or DAA. • May report to other senior management for network operational requirements.
Other	• Relies on experience and judgment to plan and accomplish goals. • Manages IA operations for an NE(s).
IA Certification	Within six months of assignment to position.

C4.4.2. Table C4.T5. lists the specific functional requirements associated with the IAM Level II position. Personnel performing these functions, regardless of their occupational title (e.g., ISSO, IAO, ISSM, logistics manager, pilot, infantry officer) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C4.T1.

Table C4.T5. IAM Level II Functional Requirements

M-II.1.	Develop, implement, and enforce policies and procedures reflecting the legislative intent of applicable laws and regulations for the NE.
M-II.2.	Prepare, distribute, and maintain plans, instructions, guidance, and standard operating procedures concerning the security of network system(s) operations.

M-II.3.	Develop NE security requirements specific to an IT acquisition for inclusion in procurement documents.
M-II.4.	Recommend resource allocations required to securely operate and maintain an organization's NE IA requirements.
M-II.5.	Participate in an IS risk assessment during the C&A process.
M-II.6.	Develop security requirements for hardware, software, and services acquisitions specific to NE IA security programs.
M-II.7.	Ensure that IA and IA enabled software, hardware, and firmware comply with appropriate NE security configuration guidelines, policies, and procedures.
M-II.8.	Assist in the gathering and preservation of evidence used in the prosecution of computer crimes.
M-II.9.	Ensure that NE IS recovery processes are monitored and that IA features and procedures are properly restored.
M-II.10.	Review IA security plans for the NE.
M-II.11.	Ensure that all IAM review items are tracked and reported.
M-II.12.	Identify alternative functional IA security strategies to address organizational NE security concerns.
M-II.13.	Ensure that IA inspections, tests, and reviews are coordinated for the NE.
M-II.14.	Review the selected security safeguards to determine that security concerns identified in the approved plan have been fully addressed.
M-II.15.	Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.
M-II.16.	Monitor contract performance and periodically review deliverables for conformance with contract requirements related to NE IA, security, and privacy.
M-II.17.	Provide leadership and direction to NE personnel by ensuring that IA security awareness, basics, literacy, and training are provided to operations personnel commensurate with their responsibilities.
M-II.18.	Develop and implement programs to ensure that systems, network, and data users are aware of, understand, and follow NE and IA policies and procedures.
M-II.19.	Advise the DAA of any changes affecting the NE IA posture.
M-II.20.	Conduct an NE physical security assessment and correct physical security weaknesses.
M-II.21.	Help prepare IA certification and accreditation documentation.
M-II.22.	Ensure that compliance monitoring occurs, and review results of such monitoring across the NE.
M-II.23.	Obtain and maintain IA certification appropriate to position.

C4.5. IAM LEVEL III

C4.5.1. IAM Level III personnel are responsible for ensuring that all enclave IS are functional and secure. They determine the enclaves' long term IA systems needs and acquisition requirements to accomplish operational objectives. They also develop and implement information security standards and procedures through the DoD certification and accreditation process. IAM Level III position requirements are listed in Table C4.T6.

Table C4.T6. IAM Level III Position Requirements

IAM Level III	
Attribute	**Level**
Experience	Usually has at least 10 years of management experience.
System Environment	Enclave Environment IAM.
Knowledge	Applies knowledge of IA policy, procedures, and workforce structure to develop, implement, and maintain a secure enclave environment.
Supervision	• Typically reports to a DAA for IA issues. • May report to other senior managers for enclave operational requirements.
Other	• Must be a U.S. Citizen. • Relies on extensive experience and judgment to plan and accomplish enclave security related goals. • Manages IA operations for an enclave(s).
IA Certification	Within six months of assignment to position.

C4.5.2. Table C4.T7. lists the specific functional requirements associated with the IAM Level III position. Personnel performing these functions, regardless of their occupational title (e.g., ISSO, IAO, ISSM, logistics manager, pilot, infantry officer) shall be identified as part of the IA workforce and must comply with the requirements in the table above and C4.T1.

Table C4.T7. IAM Level III Functional Requirements

M-III.1.	Securely integrate and apply Department/Agency missions, organization, function, policies, and procedures within the enclave.
M-III.2.	Ensure that protection and detection capabilities are acquired or developed using the IS security engineering approach and are consistent with DoD Component level IA architecture.

M-III.3.	Ensure IAT Levels I – III, IAM Levels I and II, and anyone with privileged access performing IA functions receive the necessary initial and sustaining IA training and certification(s) to carry out their IA duties.
M-III.4.	Prepare or oversee the preparation of IA certification and accreditation documentation.
M-III.5.	Participate in an IS risk assessment during the C&A process.
M-III.6.	Ensure information ownership responsibilities are established for each DoD IS and implement a role based access scheme.
M-III.7.	Analyze, develop, approve, and issue enclave IA policies.
M-III.8.	Evaluate proposals to determine if proposed security solutions effectively address enclave requirements, as detailed in solicitation documents.
M-III.9.	Identify IT security program implications of new technologies or technology upgrades.
M-III.10.	Evaluate cost benefit, economic and risk analysis in decision-making process.
M-III.11.	Interpret and/or approve security requirements relative to the capabilities of new information technologies.
M-III.12.	Interpret patterns of noncompliance to determine their impact on levels of risk and/or overall effectiveness of the enclave's IA program.
M-III.13.	Analyze identified security strategies and select the best approach or practice for the enclave.
M-III.14.	Ensure that security related provisions of the system acquisition documents meet all identified security needs.
M-III.15.	Evaluate and approve development efforts to ensure that baseline security safeguards are appropriately installed.
M-III.16.	Evaluate the presence and adequacy of security measures proposed or provided in response to requirements contained in acquisition documents.
M-III.17.	Take action as needed to ensure that accepted products meet Common Criteria requirements as stated in Reference (b).
M-III.18.	Monitor and evaluate the effectiveness of enclaves' IA security procedures and safeguards to ensure they provide the intended level of protection.
M-III.19.	Provide enclave IA guidance for development of the COOP.
M-III.20.	Ensure all IAM review items are tracked and reported.
M-III.21.	Advise the DAA of changes affecting the enclave's IA posture.
M-III.22.	Obtain and maintain IA certification appropriate to position.

C5. CHAPTER 5

DESIGNATED APPROVING AUTHORITY (DAA) REQUIREMENTS

C5.1. INTRODUCTION

C5.1.1. Reference (c) directs that a DAA be appointed for each DoD information system operating within, or on behalf of, the Department of Defense. It requires that all DAAs be U.S. citizens. They must also be DoD employees, with a level of authority allowing them to accept, in writing, the risk of operating DoD ISs under their purview. Reference (a) further requires that all DoD personnel be adequately trained and certified in order to perform the tasks associated with their IA responsibilities and makes the heads of the DoD Components responsible for ensuring that DAAs are appointed for all DoD Component ISs.

C5.1.1.1. DAA functions may be performed on a full or part time basis by a DoD civilian or military employee in the designated role.

C5.1.1.2. DAA performing other management functions such as IAM-II or IAM-III, must also meet the training and certification requirements for those categories and levels.

C5.1.2. All personnel performing DAA functions must satisfy both preparatory and sustaining DoD training and certification requirements.

C5.2. DAA FUNCTIONS AND RESPONSIBILITIES

C5.2.1. DAA Functional Description. The official with the authority to:

C5.2.1.1. Formally assume responsibility for operating a system at an acceptable level of risk.

C5.2.1.2. Establish and direct the long-term goals, policies, and procedures relating to the IS security requirements.

C5.2.1.3. Ensure that the policies, systems, and procedures comply with and support IA requirements.

C5.2.1.4. Given a final report requesting approval to operate an IS at a specified level of trust, analyze and judge the information for validity and reliability to ensure the system is able to operate at the proposed level of security.

C5.2.1.5. Review accreditation documents to confirm the level of risk is acceptable for an IS. This decision will be made by weighing the system mission requirements against the identified level of risk per DoD Instruction 5200.40 (Reference (f)) (or its successor documents) and implemented countermeasures to known vulnerabilities. Additional factors to consider include system architecture, system security measures, system operations policy, system security management plan, and provisions for system operator and end user training.

C5.2.2. Table C5.T1. lists the DAA's functional requirements.

Table C5.T1. DAA Functional Requirements

DAA.1.	Grant the authority to operate an IS or network at an acceptable level of risk.
DAA.2.	Review accreditation documents to confirm that the level of risk is within acceptable limits for each network and/or IS.
DAA.3.	Verify that each IS complies with IA requirements.
DAA.4.	Ensure establishment, administration, and coordination of security for systems that Component personnel or contractors operate.
DAA.5.	Ensure the program manager defines the system security requirements for acquisitions.
DAA.6.	Manages the IA workforce. Assigns IA responsibilities to the individuals reporting directly to the DAA.
DAA.7.	Ensures individuals filling IA positions are assigned in writing, trained, certified, and sign a statement of responsibilities.
DAA.8.	Assign the mission assurance category in accordance with References (b) and (c) for each IS and approve the classification level required for the applications implemented on them.
DAA.9.	Allocate resources to achieve and maintain an acceptable level of security and to remedy security deficiencies.
DAA.10.	Resolve issues regarding those systems requiring multiple or joint accreditation. This may require documentation of condition or agreements in Memoranda of Agreement.
DAA.11.	Ensure that, when classified or sensitive unclassified information is exchanged between ISs or networks (internal or external), the content of this communication is protected from unauthorized observation or modification by acceptable means.

C5.3. DAA TRAINING AND CERTIFICATION REQUIREMENT

C5.3.1. Each assigned DAA must:

C5.3.1.1. Complete the DoD DAA computer-based training (CBT) or web-based training (WBT) product within 60 days of assignment to the position. The CBT, titled "DAA, Designated Approving Authority," can be obtained from DoD IA Portal (formerly the Information Assurance Support Environment (IASE)).

C5.3.1.2. The DAA and the unit training officer will sign the DAA CBT certificate upon completion of the DISA DAA Certification Course (Figure C5.F1).

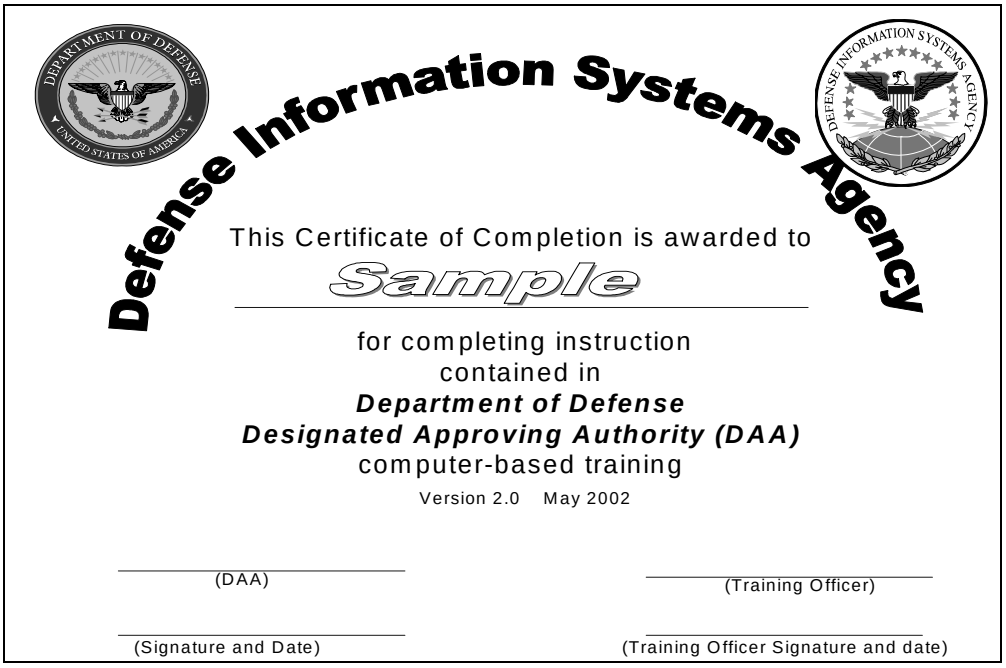
C5.3.1.3. Maintain the course completion certificate (Figure C5.F1.), also available at the DoD IA Portal, as a part of the DAA's official personnel file.

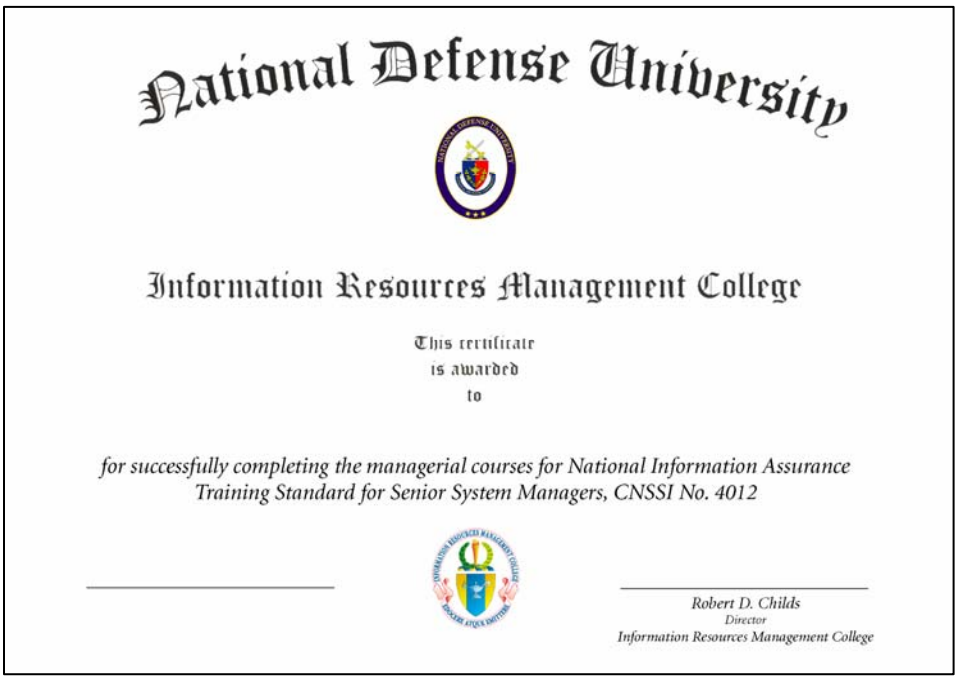
C5.3.1.4. Recertify every three years.

C5.3.2. The DAA may substitute the National Defense University/Information Resource Management College DAA course and certificate for the DISA CBT.

C5.3.3. The DoD Components are encouraged to provide additional training specific to their unique requirements.

Figure C5.F1. Sample DAA Certificate of Completion





C6. CHAPTER 6

AUTHORIZED USER MINIMUM IA ORIENTATION AND AWARENESS REQUIREMENTS

C6.1. INTRODUCTION

C6.1.1. IT has enabled the Department of Defense to transmit, communicate, collect, process, and store unprecedented amounts of information.

C6.1.2. Increasing dependence on information systems has focused attention on the need to ensure that these assets, and the information they process, are protected from actions that would jeopardize DoD's ability to effectively function.

C6.1.3. Responsibility for securing the Department's information and systems lies with the DoD Components. The trained and aware user is the first and most vital line of defense.

C6.1.4. IT users need to maintain a degree of understanding about IA policies and doctrine commensurate with their responsibilities. They must be capable of appropriately reporting and responding to suspicious activities, and know how to protect the information and IT systems to which they have access.

C6.1.5. IA orientation training must be current, engaging, and relevant to the target audience to enhance its effectiveness. Its primary purpose is to influence behavior. The focus must be on actions that empower the user 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.

C6.1.6. DISA's DoD IA Awareness CBT is the DoD 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, OMB, or the Office of the Secretary of Defense. DISA's training products can be accessed via the DoD IA Portal (formerly the IASE website).

C6.1.7. The DoD Components are expected to address organization specific topics and local incident reporting procedures.

C6.2. GENERAL REQUIREMENTS

C6.2.1 The requirements for computer security orientation and awareness training have been established under the authority of 10 U.S.C. 2224, 15 U.S.C. 278g-3, and OM&B Circular A-130 (References (g) – (i)). References (b) and (d) implement the requirements and extend it to IA.

C6.2.2. To ensure understanding of the critical importance of IA, 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.

C6.2.3. The DoD Components must document and maintain the status of orientation and awareness compliance for each user. Required versus actual IA orientation and awareness will be a management review item.

C6.2.4. All users will be informed of their information and IS security responsibilities, and consent to monitoring.

C6.2.5 At a minimum, the following themes must be conveyed in IA initial orientation and annual awareness programs:

C6.2.5.1. Critical reliance on information and IS resources.

C6.2.5.2. Commitment to protect information and IS resources.

C6.2.5.3. Threats, vulnerabilities, and related risks associated with IS.

C6.2.5.4. Consequences for inadequate protection of the organization's IS resources.

C6.2.5.5. The essential role of the DoD employee.

C6.3. SPECIFIC REQUIREMENTS

User orientation and awareness programs will address:

C6.3.1. The importance of IA to the organization and to the authorized user.

C6.3.2. Relevant laws, policies, and procedures, and how they affect the authorized user (e.g., copyright, ethics, standards of conduct).

C6.3.3. Examples of external threats such as script kiddies, crackers, hackers, protesters, or agents in the employ of terrorist groups or foreign countries.

C6.3.4. Examples of internal threats such as malicious or incompetent authorized users, users in the employ of terrorist groups or foreign countries, disgruntled employees or service members, hackers, crackers, and self-inflicted intentional or unintentional damage.

C6.3.5. The potential elevated sensitivity level of aggregated unclassified information.

C6.3.6. Authorized user risk from social engineering.

C6.3.7. Common methods to protect critical system information and procedures.

C6.3.8. Principles of shared risk in networked systems (i.e., how a risk assumed by one person is imposed on the entire network) and changes in the physical environment (e.g. water, fire, dust/dirt).

C6.3.9. Risks associated with remote access (e.g., telecommuting, during deployment, or on temporary duty).

C6.3.10. Legal requirements regarding privacy issues, such as email status (DoD Directive 2500 (Reference (j)) and the need to protect systems containing payroll, medical and personnel records.

C6.3.11. Knowledge of malicious codes (e.g., logic bomb, Trojan horse, malicious mobile code, viruses, and worms) including how they attack, how they damage an IS, how they may be introduced inadvertently or intentionally, and how users can mitigate their impact.

C6.3.12. The impact of distributed denial of service attacks and what users can do to mitigate them.

C6.3.13. How to prevent self-inflicted damage to system information security through disciplined application of IA procedures such as proper log on, use of passwords, preventing spillage of classified information, e-mail security, etc.

C6.3.14. Embedded software and hardware vulnerabilities, how the Department of Defense corrects them (e.g., IAVA process), and the impact on the authorized user.

C6.3.15. Prohibited or unauthorized activity on DoD systems (e.g., peer-to-peer file sharing, gambling, personal use and gain issues).

C6.3.16. Requirements and procedures for reporting spillages, unauthorized or suspicious activity, and local IA office point of contact information.

C6.3.17. Categories of information classification and differences between handling information on the Non-Classified Internet Protocol Router Network (NIPRNet) or the SECRET Internet Protocol Router Network (SIPRNet).

C6.3.18. Software issues including license restrictions on DoD systems, encryption, and media sanitation requirements and procedures.

C6.3.19. Definition of Information Operations Condition (INFOCON) and its impact on authorized users.

C6.3.20. Sources of additional information and training.

C7. CHAPTER 7

IA WORKFORCE IDENTIFICATION, TRACKING, AND ASSIGNMENT

C7.1. INTRODUCTION

C7.1.1. The Department of Defense must manage its IA workforce effectively and efficiently to provide trained, skilled personnel who will protect the operation of its IS.

C7.1.2. The DoD Components will leverage existing manpower and personnel databases, learning management systems, other tools, and procedures to support effective management of their IA workforces.

C7.1.3. Tools and procedures must enable the assignment and tracking of qualified personnel both within the DoD Components and in support of joint assignments.

C7.1.4. As a prerequisite to effective IA management, the DoD Components must identify all positions and personnel with IA responsibilities, regardless of occupational specialty, or whether the duty is performed as primary or as an additional/embedded duty. Positions and personnel will be aligned to an IA category and level, per Chapters 3-5, and documented in the appropriate database(s). IA Workforce data elements must comply with requirements established in Reference (b) and DoD Instruction 7730.64, DoD Instruction 1336.5, and Dod instruction (References (k), (l), and (m)).

C7.1.5. The DoD Components must use, to the extent possible, existing personnel/manpower and unit organizational databases to satisfy the requirements outlined in this chapter. These include, but are not limited to, the Defense Civilian Personnel Data System (DCPDS) and the Defense Integrated Military Human Resources System (DIMHRS). Until the DIMHRS can meet the requirement, the DoD Components are responsible for providing this information per References (l) and (m) for military members. DoD Instruction 1444.2 (Reference (n)) dictates DoD civilian database requirements.

C7.1.6. The Defense Manpower Data Center (DMDC) will leverage DoD Component provided information on civilian and military IA positions and personnel to support development of an integrated picture of the DoD IA workforce per Chapter 8 and References (b), (k), (l), (m) and (n).

C7.2. IA WORKFORCE MANAGEMENT

C7.2.1. The DoD Components must identify military, civilian, and contractor personnel performing IA functions whether performed as their primary duty, or as an additional/embedded duty. Chapters 3, 4, and 5 provide a DoD standard naming convention and descriptions of IA categories, levels, and their related functions.

C7.2.2. Identify all positions required to perform IA functions, by category and level, in manpower tables of organization. Identification of the IA workforce positions must be a management review item.

C7.2.3. Assign appropriately trained and certified personnel to IA positions (internal and joint positions), per Chapters 2-5.

C7.2.4. Require each individual assigned IA responsibilities to sign a statement of responsibilities appropriate for that position. Appendix 4 provides a recommended statement of responsibilities for privileged access users.

C7.2.5. Track IA personnel training and certification against position requirements. Positions performing both management and technical functions must be identified individually in the appropriate manpower database. Personnel filling these positions must be aligned with both positions and maintain the appropriate certification/qualifications for each.

C7.2.6. Report on DoD Component training (including awareness) and certification programs in accordance with Chapter 8.

C7.3. IA WORKFORCE IDENTIFICATION REQUIREMENTS

C7.3.1. To manage the IA workforce effectively, the DoD Components must comply with the following requirements for each employee group.

C7.3.2. Civilians:

C7.3.2.1. DoD personnel in the 2210 job series shall be classified by parenthetical title. They must indicate a primary parenthetical title based on the position's primary or paramount duties. They must also indicate a secondary title if performing additional/embedded duties beyond those primary duties even if they could be considered a "Generalist" per Reference (o).

C7.3.2.2. Identify all civilian positions and personnel required to perform IA functions described in this Manual in the appropriate database(s) (e.g., DCPDS, Joint Manpower and Personnel System (e-JMAPS), or equivalent), including Local Nationals, performing IA functions, regardless of series, and align with the categories and levels described in Chapters 3-5.

C7.3.2.2.1. All IA positions, regardless of whether IA functions are performed as a primary duty or as an additional/embedded duty.

C7.3.2.2.2. All personnel, including LNs, performing IA functions.

C7.3.2.2.3. Certification status of incumbent including certification or recertification date, cost of certification/recertification test, and associated training (if paid by the government).

C7.3.2.2.4. Waivers granted for personnel filling IA positions.

C7.3.2.3. Verify that DCPDS or equivalent has the correct data (down to the specialty level for the 2210 series).

C7.3.2.4. Special civilian titling and DCPDS reporting requirements across the Department of Defense:

C7.3.2.4.1. The DoD Components must use the existing authorized parenthetical title for Security, "INFOSEC," to support IA workforce identification and management requirements across the Department of Defense. The DoD Components will ensure that DCPDS reflects the following guidance:

C7.3.2.4.2. All positions in the 2210 job series must comply with the Office of Personnel Management (OPM) guidance on standardized titling. Positions in the 2210 job series with primary or additional/embedded IA functions must enter the authorized parenthetical title for Security, "INFOSEC," in DCPDS.

C7.3.2.4.3. Position Specialty Code (PSC): The DoD Components must ensure that all DoD civilian positions and personnel with IA functions, regardless of OPM series or job title, use "INFOSEC" as the Position Specialty Code (PSC) in the Defense Civilian Personnel Data System. The PSC allows identification of a DoD civilian position with IA functions regardless of OPM series or job title. The abbreviation for Security, "INFOSEC," established in this Manual, supports civilian IA workforce identification and management requirements across the Department of Defense.

C7.3.3. Military:

C7.3.3.1. Identify all military positions and personnel required to perform IA functions described in this Manual in the appropriate database(s) (e.g., e-JMAPS, DIMHRS, or Component Manpower/Personnel Systems), including Foreign Nationals, regardless of occupational specialty, and align with the categories and levels described in Chapters 3-5.

C7.3.3.2. Identify the following, regardless of occupational specialty, in DIMHRS, eJMAPS, or the DoD Component manpower and/or personnel management systems, as appropriate:

C7.3.3.2.1. All IA positions, regardless of whether IA responsibilities are performed as a primary duty or as an additional/embedded duty.

C7.3.3.2.2. All personnel performing IA functions.

C7.3.3.2.3. Certification status of incumbent including certification or recertification date, cost of certification/recertification test, and associated training (if paid by the government).

C7.3.3.3. Assign a code to each IA position that identifies its category and level, and the corresponding minimum certification requirements per Chapters 3-5 and Appendix 4.

C7.3.3.4. Assign a code to individuals based on their certification level.

C7.3.3.5. Match the certified individuals against required positions.

C7.3.3.6. Track the IA workforce against the required positions.

C7.3.4. Contractors

C7.3.4.1. Identify all contractors performing IA functions and align with the categories and levels described in Chapters 3 and 4.

C7.3.4.2. Ensure that contractor personnel, including LNs, have the appropriate IA certification and background investigation.

C7.3.4.3. Ensure the capability to report in detail on individual contractor employee certification(s) and certification status.

C7.3.4.4. Specify contractor certification and training requirements in all contracts that include acquisition of IA services. Eligible contractor personnel must have their IA certification and function level documented in the Defense Enrollment Eligibility Reporting System (DEERS).

C7.3.4.5. Contracting officers' technical representatives will enter the required data into a DMDC application which will feed into DEERS.

C8. CHAPTER 8

IA WORKFORCE MANAGEMENT REPORTING AND METRICS

C8.1. INTRODUCTION

C8.1.1. To manage its IA workforce effectively and efficiently, and provide trained and certified personnel when and where needed, the Department of Defense must know IA position requirements, the existing IA workforce and its qualifications, and where these critical assets are employed.

C8.1.2. The reporting requirements and metrics outlined in this chapter support DoD's current and long-term management of critical IA personnel resources.

C8.1.3. The DoD Components must use, to the extent possible, existing personnel/manpower/unit organizational databases and tools to satisfy these IA reporting requirements.

C8.1.4. The IA Training and Certification Program annual report is due and covers the same reporting period as the Federal Information Security Management Act (FISMA) report, Reference (p). The IA Training and Certification Program report consolidates IA training, certification, and workforce management reporting requirements per References (a)-(e).

C8.2. REPORTING REQUIREMENTS

C8.2.1. ASD(NII)/DoD CIO coordinates IA Training and Certification Program reporting requirements, and ensures that collected information supports ASD(NII)/DoD CIO validation of DoD IA workforce readiness. Figure C8.F1. provides the basic IA workforce information the DoD Components will track and report.

C8.2.2. All the DoD Components are required to submit data on the status of their IA workforce for inclusion in the IA annual report.

C8.2.3. The DoD Components will provide both qualitative and quantitative information. The information reported will support the following IA workforce management critical information requirements:

C8.2.3.1. Methodologies used to identify employees required to perform IA functions.

C8.2.3.2. Training and certification requirements developed by the Components for employees performing IA functions.

C8.2.3.3. Tracking processes used to determine requirements for how many employees perform IA functions and have received IA training and certification.

C8.2.3.4. Plans and methodologies to track, monitor, and document completion of IA orientation and awareness training for all network users.

C8.2.3.5. The ASD(NII)/DoD CIO will review and validate/approve the methodologies and processes reported by the Components to implement and maintain the DoD baseline requirements of this Manual.

C8.2.4. ASD(NII)/DoD CIO will combine data from the DoD Components to assemble a consolidated annual IA Workforce Training, Certification, and Management report. The annual report will include DoD Component comments regarding IA workforce lessons learned, issues from the previous calendar year (coordinated with FISMA reporting dates), and plans for the next. It will also provide statistics for personnel performing IA functions on a primary or additional/embedded duty basis, broken down by IA category and level.

C8.2.5. In addition to the reporting requirements outlined in this chapter, ASD(NII)/DoD CIO will gather data on numerous aspects of the IA workforce including recruitment, retention, training, and impact on IA operations. This data will be combined with the DoD Component submitted reports to develop a comprehensive picture of the IA workforce and its operational effectiveness.

C8.2.6. Qualitative Requirements:

C8.2.6.1. The DoD Components will describe the methodologies, requirements, and processes used to implement requirements of Reference (a) and this Manual. Specifically, Components will report:

C8.2.6.1.1. Methodologies used to identify employees in the Information Assurance workforce.

C8.2.6.1.2. Training and certification requirements developed for employees in the IA workforce such as:

C8.2.6.1.2.1. DoD Component schools/training centers IA-related curriculum status and actual/planned annual throughput. Highlight accomplishments and initiatives; describe any partnerships/cooperative arrangements with other DoD entities, and/or the private sector (i.e., industry and academia) regarding IA curriculum program activities.

C8.2.6.1.2.2. Component specific training and certification requirement including the operating system requirement in addition to the DoD baseline requirements.

C8.2.6.1.2.3. Programs to train and certify personnel performing IA functions. Highlight key features (e.g., needs self-assessment) and accomplishments to include number and percent of total participants completing training and certified.

C8.2.6.1.3. Tracking processes used to determine how many employees are in the IA workforce and properly certified and have received required training.

C8.2.6.1.4. Status of recruitment and retention for the IA workforce, indicating if it is increasing, stable, or decreasing, and why.

C8.2.6.1.5. Plans and methodologies used to track, monitor, and document completion of IA orientation and awareness training for all network users.

C8.2.6.1.6. Programs for IA orientation and awareness in the workforce. Highlight key features of the program and major accomplishments.

C8.2.6.1.7. Provide evidence to substantiate/explain reported completion rates for the IA orientation and awareness program requirement.

C8.2.6.1.8. IA curriculum/treatment in CAPSTONE, officer accession programs, Flag, Commanding Officer/Executive Officer, and Warrant Officer indoctrination and component professional military education courses, as applicable including resident, distributive, and blended.

C8.2.6.1.9. Defense/service colleges, universities, and professional military education. IA related curriculum, its status, and actual/planned annual throughput, including resident, distributive, and/or blended. Highlight any IA related accomplishments and initiatives; including partnerships/cooperative arrangements with other DoD entities, and/or the private sector (i.e., industry, academia).

C8.2.7. Quantitative Data Requirements:

C8.2.7.1. Each DoD Component must ensure that its personnel and staffing databases are properly configured, per References (k)-(n), to capture the following quantitative data. If a given metric cannot be captured to a database, it must be reported manually, and included with the submission of qualitative data described above.

C8.2.7.2. IA workforce positions and manning status. (This is a management review item.)

C8.2.7.2.1. Number of IA positions, by category and level.

C8.2.7.2.1.1. Primary duty IA positions.

C8.2.7.2.1.2. Additional/embedded duty IA positions.

C8.2.7.2.2. Number of IA positions filled, by category, and level.

C8.2.7.2.3. Number of IA positions filled with certified incumbents by category and level.

C8.2.7.3. Personnel certification levels: (This is a management review item.)

C8.2.7.3.1. Number of personnel certified, by category and level.

C8.2.7.3.2. Number of personnel certified, by category and level who are actually filling an IA position.

C8.2.7.3.3. Recertification rates -- number of personnel who were recertified during the current year.

C827.3.4. Number of waivers granted for personnel filling IA positions.

C8.2.7.4. Total dollars obligated or expended for IA training and certification (including courses leading to certification).

C8.2.7.5. Compliance with workforce certification continuing education and sustainment training requirement

C8.2.7.6. Number of users who completed IA orientation and awareness training requirement versus total number of authorized users. (This is a management review item.)

C8.2.8. IA Workforce Annual Report Instructions:

Instructions: Each DoD Component must provide to DMDC relevant required data to populate these tables for the preceding calendar year. The report/data is due to the ASD(NII)/DoD CIO annually, and the due date will be coordinated with the FISMA Report Requirement. DMDC will create a consolidated report capturing the DoD Component's IA Workforce Data reflected in the tables below. **(Note:** LNs are included in two employee groups: Civilian and Contractor. LN includes all individuals working for the Department of Defense in a foreign country who are nationals or non U.S. residents of that country.)

Figure C8.F1. IA Workforce Annual Report Format

Table 1: IA Workforce Primary Duty Positions

	Civilian			Military			Contractor	
	Number	Filled	Certified*/ Waiver	Number	Filled	Certified*/ Waiver	Filled	Certified* /Waiver
IAT I								
IAT II								
IAT III								
IAM I								
IAM II								
IAM III								
Total								

* Certified in accordance with the policy for that position. Waivers must be approved by the DAA (see paragraph C3.2.4.2., C3.2.4.3., C4.2.3.2., or C4.2.3.4.2. Count personnel filling both IAT and IAM Category positions in both categories per C2.2.5. and AP2.1.2.3.

Table 2: IA Workforce Additional/Embedded Duty Positions

	Civilian			Military			Contractor	
	Number	Filled	Certified*/ Waiver	Number	Filled	Certified*/ Waiver	Filled	Certified*/ Waiver
IAT I								
IAT II								
IAT III								
IAM I								
IAM II								
IAM III								
Total								

* Certified in accordance with the policy for that position. Waivers must be approved by the DAA (see paragraph C3.2.4.2., C3.2.4.3., C4.2.3.2., or C4.2.3.4.2. Count personnel filling both IAT and IAM Category positions in both categories per C2.2.5. and AP2.1.2.3.

Table 3: IA Workforce Certification/Recertification

	Civilian		Military		Contractor	
	Required	Recertified	Required	Recertified	Required	Recertified
IAT I						
IAT II						
IAT III						
IAM I						
IAM II						
IAM III						
Total						

C8.2.9. The Information Assurance Training and Certification Program annual report has been assigned report control symbol DD-NII(A)XXXX in accordance with DoD 8910.1-M (Reference (q)).

C9. CHAPTER 9

IA WORKFORCE IMPLEMENTATION REQUIREMENTS

C9.1. INTRODUCTION

C9.1.1. This chapter provides guidance to support a coordinated and orderly transition from the legacy systems and processes to full compliance with DoD's requirements. These actions require in-depth budget and personnel management planning.

C9.1.2. Adhering to the categories and levels outlined is critical to support the effective identification of the IA workforce across the Department of Defense. Standardizing skill sets supports joint assignments and system interoperability.

C9.2. GENERAL REQUIREMENTS

C9.2.1. The DoD Components must:

C9.2.1.1. Plan for, and incrementally complete, these requirements over four years from the effective date of this Manual.

C9.2.1.2. Develop and submit to the Council implementation policies, processes, and plans to support compliance with the requirements outlined below within six months of the publication date of this Manual.

C9.2.1.3. Provide representation to the Council as required in Chapter 1.

C9.2.1.4. Report progress annually, against implementation requirements, to ASD(NII)/DoD CIO , using the format presented in Figure C9.F1.

C9.3. SPECIFIC REQUIREMENTS

C9.3.1. To allow for proper identification and planning of requirements, the Department of Defense has adopted a phased approach to this implementation. The first year provides time for the identification of specific requirements to support budget and staffing planning, and to certify the initial 10 percent of the IA workforce. The next three years provide time to bring the full IA workforce into compliance with the requirements in phases. Thirty percent of the workforce must come into compliance each year, as outlined below.

C9.3.2. Within 12 months of the effective date of this Manual, the DoD Components must:

C9.3.2.1. Provide Component IAM and Human Resource Management participation in the DoD sponsored Component Implementation Workshop that will be conducted by the Defense-wide Information Assurance Program (DIAP) Office within three months of publication of this Manual.

C9.3.2.2. Identify all positions per Chapters 3-5 and 7, required to execute the IA functions listed in Chapters 3-5 as primary or additional/embedded duties.

C9.3.2.3. Assign IA workforce Category and Level codes for the Component's staffing and personnel data systems based on the categories and levels described in Chapters 3-5. These codes must be identified to DMDC per Reference (k). The data elements will be routinely captured by the DMDC and formatted to support the DoD's IA workforce management requirements. If a Component uses a personnel or manpower system or database that does not exchange data with DMDC systems, develop the necessary data fields to track IA workforce requirements.

C9.3.2.4. Budget for IA training, certification, and workforce management requirements of DoD government personnel, as described below. The budget plan must ensure implementation of the requirements over a three year period, and must specifically include resources for:

C9.3.2.4.1. Staffing identified IA positions (primary or additional/embedded duty).

C9.3.2.4.2 Training incumbents.

C9.3.2.4.3. Ensuring staffing and unit databases/tools are upgraded to support IA workforce management requirements as appropriate.

C9.3.2.4.4. Training for staffing managers on the systems and processes required to support the IA workforce training and management requirements.

C9.3.2.4.5. Certifying (including training and testing) current and planned IA workforce members.

C9.3.2.5. The DoD Components must plan to meet the following milestones. The milestone plan will begin with the next planning, program, and budget cycle to execute these requirements beginning in FY-07. The phases of this implementation approach are:

C9.3.2.5.1. Year One (FY-06): Identify IA workforce positions, fill 10 percent of the IA positions with certified personnel. Develop budget to support follow-on implementation years two–four.

C9.3.2.5.2. Year Two: Fill a total of 40 percent of the IA positions with certified personnel.

C9.3.2.5.3. Year Three: Fill a total of 70 percent of the IA positions with certified personnel.

C9.3.2.5.4. Year Four: All filled IA positions are held by certified personnel.

C9.3.2.5.5. Thereafter, all incumbents and new hires must be trained, certified, and recertified in accordance with this Manual.

C9.4. IMPLEMENTATION PLAN REPORTING REQUIREMENTS

C9.4.1. The DoD Components must report progress to ASD(NII)/DoD CIO on budgeting to meet implementation requirements using the format in Figure C9.F1. The Information Assurance Workforce Milestone Budget Plan Report is exempt from licensing in accordance with the provisions of paragraph C4.4.6. of Reference (q).

C9.4.2. The IA Workforce Implementation Milestone Budget Plan report is due 31 July each year for five years from the date of publication of this Manual.

Figure C9.F1. IA Workforce Milestone Budget Plan Report

IA Workforce Milestone Budget Plans (training and certification, costs)								
IA WF Budget	**PY**	**CY**	**BY00**	**BY01**	**BY02**	**BY03**	**BY04**	**Total**
Required								
Budgeted								
Obligated								

PY=Previous Year, CY=Current Year, BY=Budget Year

AP1. APPENDIX 1

AP1. DEFINITIONS

AP1.1. Authorized User. Any appropriately cleared individual required to access a DoD IS to carry out or assist in a lawful and authorized governmental function. Authorized users include DoD employees, contractors, and guest researchers.

AP1.2. Categories, Levels, and Functions. The structure for identifying all DoD Information Assurance (IA) positions and personnel.

AP1.2.1. Categories. The DoD IA workforce is split into two major categories of Technical and Management. Management refers to personnel performing any IAM functions described in Chapters 4 or 5.

AP1.2.2. Levels. Each of the IA workforce categories has three levels (Technical or Management Level I, II, and III). The management category also includes the Designated Approving Authority (DAA) position.

AP1.2.3. Functions. High level tasks required to successfully perform IA for an information system. The function indicates the tasks that an employee performs or occupational requirements to successfully perform as part of the IA Workforce. For the purposes of this Manual the IA functions have been associated with a category and level. These functions provide a means to distinguish between different levels of work. The functional level approach also encourages a broader, more integrated means of identifying what an employee must know to perform the tasks that comprise an IA position across all of the DoD Components.

AP1.3. Certification. Recognition given to individuals who have met predetermined qualifications set by an agency of government, industry, or profession. Certification provides verification of individuals' knowledge and experience through evaluation and approval, based on a set of standards for a specific profession or occupation's functional job levels. Each certification is designed to stand on its own, and represents an individual's mastery of a particular set of knowledge and skills.

AP1.4. Computing Environment (CE). Local area network(s) server host and its operating system, peripherals, and applications.

AP1.5. Contractor. Per the Defense Acquisition University Glossary, "an entity in private industry which enters into contracts with the government to provide goods or services." For DoD IA purposes, an entity is a private sector employee performing IA functions in support of a DoD IS. Private sector employees performing IA functions must meet the same standards for system access or management as government IA employees.

AP1.6. Defense Civilian Personnel Data System (DCPDS). DCPDS is a human resources transaction IS supporting civilian personnel operations in the Department of Defense. DCPDS is

designed to support appropriated fund, non-appropriated fund, and LN human resources operations.

AP1.6.1. The Corporate Management Information System (CMIS) consolidates DoD employee and position data for all DoD civilian employees from all DCPDS databases to provide a corporate level data query and reporting capability.

AP1.6.2. DCPDS and CMIS support strategic DoD civilian workforce planning, trend analysis, mobilization, and contingency planning.

AP1.7. Designated Approving Authority (DAA). The official with the authority to formally assume responsibility for operating a system at an acceptable level of risk. This term is synonymous with Designated Accrediting Authority and Delegated Accrediting Authority defined by the Committee on National Security Systems Instruction No. 4009 (Reference (r)).

AP1.8. DoD Information System (IS). Includes automated IS (AIS) applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

AP1.8.1. An AIS application performs clearly defined functions for which there are readily identifiable security considerations and needs addressed as part of the acquisition. An AIS application may be a single software application (e.g., Integrated Consumable Items Support), multiple software applications related to a single mission (e.g., payroll or personnel), or a combination of software and hardware performing a specific support function across a range of missions (e.g., Global Command and Control System, Defense Messaging System). AIS applications are deployed to enclaves for operations and have their operational security needs assumed by the enclave.

AP1.8.1.1. Note: An AIS application is analogous to a “major application,” as defined in OMB A-130 (Reference (i)). However, to avoid confusion with the DoD acquisition category called “Major Automated Information System”, this term (AIS) is not used in this Manual.

AP1.8.2. Defense Integrated Military Human Resources System (DIMHRS). A system being designed which will provide a fully integrated personnel and pay system for all of the Military Services. This system will include personnel tracking and management functionality.

AP1.9. Duty

AP1.9.1. Primary. An IA position with primary duties focused on IA functions. The position may have other duties assigned, but the main effort focuses on IA functions. The position would normally require at least 25 to 40(+) hours per week devoted to IA functions.

AP1.9.2. Additional. A position requiring a significant portion of the incumbent’s attention and energies to be focused on IA functions, but in which IA functions are not the primary responsibility. The position would normally require 15 to 24 hours, out of a 40(+) hour week, devoted to IA functions.

AP1.9.3. Embedded. A position with IA functions identified as an integral part of other major assigned duties. These positions normally require up to 14 hours, out of a 40(+) hour week be devoted to IA related functions.

AP1.10. Eligible DoD Contractors. An employee or individual under contract or subcontract to the Department of Defense, designated as providing services or support to the Department that requires logical and/or physical access to the Department's assets.

AP1.11. Enclave. Collection of CE connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves provide standard IA capabilities such as boundary defense, incident detection and response, and key management, and also deliver common applications such as office automation and electronic mail. Enclaves are analogous to general support systems, as defined in OMB A-130 (Reference (i)). Enclaves may be specific to an organization or a mission and the CE may be organized by physical proximity or by function, independent of location. Examples of enclaves include local area networks and the applications they host, backbone networks, and data processing centers.

AP1.12. Foreign National. Individuals who are non-U.S. citizens including U.S. military personnel, DoD civilian employees, and contractors.

AP1.13. General Schedule (GS)/Pay Band. The Office of Personnel Management's basic classification and compensation system for white collar occupations in the Federal government, as established by 5 U.S.C. 51 (Reference (s)).

AP1.13.1. Job Series. A subgroup of an occupational group or job family that includes all classes of positions at the various levels in a particular kind of work, such as the GS-2210 series. Positions within a series are similar in subject matter, basic knowledge and skill requirements.

AP1.13.2. Parenthetical Specialty. A subset of work within a series distinguishing positions on the basis of specialized technical requirements. The 2210 series has officially designated parenthetical specialties that agencies must include in official position titles. "INFOSEC" is the parenthetical specialty used in DCPDS for 2210 employees performing security (IA) functions.

AP1.13.3. Position Specialty Code. A unique DoD civilian workforce code to support effective management of the IA workforce. The position specialty code identifies a DoD civilian position, or person with IA functions, regardless of OPM job series.

AP1.14. 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.

AP1.15. Information Assurance Workforce. The IA workforce focuses on the operation and management of IA capabilities for DoD systems and networks. The workforce ensures adequate security measures and established IA policies and procedures are applied to all ISs and networks. The IA workforce includes anyone with privileged access and IA managers who perform any of the responsibilities or functions described in Chapters 3-5. The DoD IA Workforce includes but is not limited to all individuals performing any of the IA functions described in this Manual. Additionally the IA workforce categories/functions will be expanded to include (for example) system architecture and engineering, computer network defense, certification and accreditation, and vulnerability assessment as changes to this Manual. These individuals are considered to have significant "security responsibilities" and must receive specialized training and be reported per Reference (p) and this Manual.

AP1.16. Information Assurance Vulnerability Alert (IAVA). The comprehensive distribution process for notifying the Components about vulnerability alerts and countermeasures information.

AP1.17. Information Assurance Vulnerability Management (IAVM). The IAVM process provides positive control of the vulnerability notification process for DoD network assets. The IAVM requires COMPONENTS receipt acknowledgment and provides specific time parameters for implementing appropriate countermeasures, depending on the criticality of the vulnerability.

AP1.18. Information Operations Condition (INFOCON). A comprehensive defense posture and response based on the status of ISs, military operations, and intelligence assessments of adversary capabilities and intent.

AP1.19. Local National Employee. Civilians or contractors, whether paid from appropriated or non-appropriated funds, employed or used by U.S. Forces in a foreign country who are nationals or non-U.S. residents of that country.

AP1.20. Network Environment (Computer). The constituent element of an enclave responsible for connecting CE by providing short haul data transport capabilities, such as local or campus area networks, or long haul data transport capabilities, such as operational, metropolitan, or wide area and backbone networks that provides for the application of IA controls.

AP1.21. 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 information assurance.

AP1.22. Privileged Access. An authorized user who has access to system control, monitoring, administration, criminal investigation, or compliance functions. Privileged access typically provides access to the following system controls:

AP1.22.1. Access to the control functions of the information system/network, administration of user accounts, etc.

AP1.22.2. Access to change control parameters (e.g., routing tables, path priorities, addresses) of routers, multiplexers, and other key information system/network equipment or software.

AP1.22.3. Ability and authority to control and change program files and other users' access to data.

AP1.22.4. Direct access to operating system level functions (also called unmediated access) that would permit system controls to be bypassed or changed.

AP1.22.5. Access and authority for installing, configuring, monitoring, or troubleshooting the security monitoring functions of information systems/networks (e.g., network/system analyzers; intrusion detection software; firewalls) or in performance of cyber/network defense operations.

AP1.23. Red Team. An independent and focused threat-based effort by a multi-disciplinary, opposing force using active and passive capabilities; based on formal; time-bounded tasking to expose and exploit information operations vulnerabilities of friendly forces as a means to improve readiness of U.S. units, organizations, and facilities.

AP1.24. Supporting IA Infrastructures. Collections of interrelated processes, systems, and networks providing a continuous flow of information assurance services throughout the Department of Defense (e.g., the key management infrastructure or the incident detection and response infrastructure).

AP1.25. Training

AP1.25.1. Resident. Instructor led classroom instruction based on specific performance criteria.

AP1.25.2. Distributive. Computer-based training (CBT) via website, computer disc, or other electronic media.

AP1.25.3. On-the-job training (OJT). Supervised hands on training, based on specific performance criteria that must be demonstrated to a qualified supervisor.

AP1.25.4. Blended: A combination of instructor-led classroom training and distributed media. This may also include instructor-led classroom training using distributed multi-media.

AP1.26. Waivers

AP1.26.1. DAAs may waive the IAT or IAM certification requirement(s) under severe operational or personnel constraints. The waiver must be documented by the DAA using a memorandum for the record stating the reason for the waiver and the plan to rectify the constraint. Waivers must be time limited, NOT TO EXCEED SIX MONTHS, and include an expiration date. Uncertified IAT Level Is are not authorized unsupervised privileged access until fully qualified per Chapter 3.

AP1.26.2. Waivers for IAT Level I certification requirements are not authorized for personnel deployed to a combat theatre of operations. The DAA may approve a waiver for certified IAT-Is to fill level IAT-II or IAT-III billets while deployed in a combat environment without attaining the appropriate certification. The DAA may grant an interim waiver limited to the period of the deployment. The interim waiver places an individual in a suspense status and must be time limited and include an expiration date not to exceed six months following date of return from combat status. The DAA may also authorize waivers for certified IAM-Is or IAM IIs to fill higher management positions in combat zones.

APPENDIX 2

AP2. IA WORKFORCE LEVELS, FUNCTIONS AND CERTIFICATION APPROVAL PROCESS

AP2.1. CERTIFICATION CRITERIA

AP2.1.1. The list of certifications contained in Table AP3.T1. is approved for the DoD IA workforce as of the publication date of this Manual.

AP2.1.2. The table maps the certifications to the IA categories and levels to which they apply.

AP2.1.2.1. IA personnel must obtain and maintain a certification corresponding to the highest level function(s) they perform.

AP2.1.2.2. Individuals performing IAT functions must hold, at a minimum, an IAT Level I certification, before gaining privileged access to any DoD system.

AP2.1.2.3. Individuals performing both IAT and IAM category functions must hold certifications appropriate to the functions performed in each category.

AP2.1.3. Commercial, vendor specific, or component developed equivalent certifications approved for the DoD IA workforce requirement must align to the IA functional requirements. Additionally, to ensure validity, certifications must be accredited and maintain accreditation under the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 17024 "General Requirements for Bodies Operating Certification of Persons," April 2003 ISO/IEC 17024 Standard, Reference (t), and be approved by the Council.

AP2.2. CERTIFICATION REVIEW PROCESS

AP2.2.1. The list of approved IA certifications must be reviewed at least annually to ensure continued applicability to the Department of Defense. Certifications may be government or commercially granted, but must be accredited to the requirements of Reference (t). Currently, not all certifications listed in this Manual meet this standard. Each has submitted a letter of intent to do so within two years from the publication date of this Manual. Certifications not accredited to the ISO standard within two years cannot be used to meet the DoD IA security standard. However, they may, if appropriate, be used to meet Component local operating system requirements.

AP2.2.2. The Office of the DoD DCIO will charter and chair the Council to maintain the IA workforce categories, levels, functions, and certifications. The Council must meet periodically to approve, remove, and assign certifications to the appropriate IA workforce levels.

AP2.2.3. Appendix 3 will be updated and reissued as needed to reflect the results of this review process.

APPENDIX 3

AP3. IA WORKFORCE CERTIFICATIONS

AP3.1. Each cell within the matrix provides a list of the DoD approved certifications aligned to each category and level of the IA workforce. Personnal performing IA functions must obtain one of the certifications required for their positions's category and level. DoD Components may choose one of the approved certifications as that Component's standard for each category and level of the IA workforce. Components may choose any approved certification to meet the requirements for the associated level for which the certification has been approved.

AP3.1.1. Each cell contains the name of the organization that sponsors the certification. These may be commercial, government, or other entities whose certification meets the requirements for the IA functional level(s) represented by the cell.

AP3.1.2. A certification may apply to more than one level.

AP3.1.3. Most IA levels within a category have more than one approved certification.

AP3.1.4. An individual needs to obtain only one of the “approved certifications” for his or her IA category and level to meet the minimum requirement. For example, an individual in an IAT Level II position could obtain any one of the four certifications listed in the corresponding cell.

AP3.1.4.1. IAT Level certifications are cumulative. Higher level certifications qualify for lower level requirements. Certifications listed in Level II or III cells can be used to qualify for Level I. However, Level I certifications cannot be used for Level II or III unless the certification is also listed in the Level II or III cell. For example:

AP3.1.4.1.1.. The A+ or Network+ certification qualify only for Technical Level I and could not be used for Technical Level II positions.

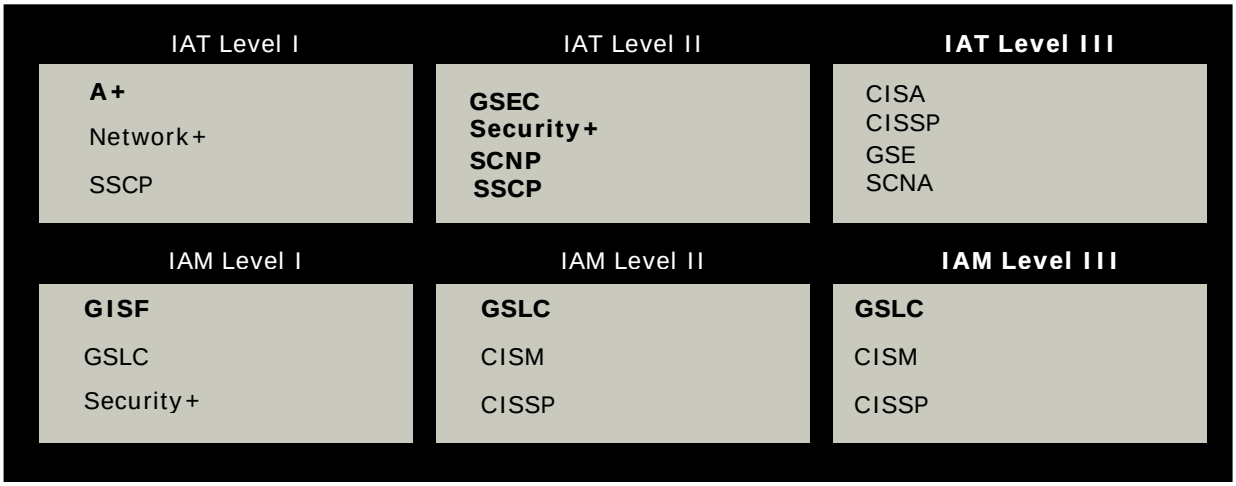
AP3.1.4.1.2. The SSCP certification qualifies for both Technical Level I and Technical Level II. If the individual holding this certification moved from an IAT Level I to an IAT Level II position, he or she would not have to take a new certification.

AP3.1.5. Management certifications corresponding to the position level do not cascade down. Each position requires the individual to meet one of the specific certifications associated with that Management Level. An IAM I must obtain one of certifications shown in the IAM I box such as the Security +. The IAM I should not take the CISSP unless already qualified in one of the certifications listed in the IAM I box (e.g., Security +).

AP3.1.6. Operating System Requirement. IATs must also obtain certifications required to implement the IA requirements for their specific operating system environment (e.g., Microsoft Operating Systems Administrator Certification), unless the operating system certification is also on the list of approved DoD IA Certifications at Table AP3.T1.

This table lists the commercial certifications and the organization that sponsors that certification**.**

Table AP3.T1. DoD Approved Baseline Certifications



.

Technical level individuals must also be certified in their CE.

Table AP3.T2. IA Workforce Certification Organizations

Certification Provider	**Certification Name**
Computing Technology Industry Association (CompTIA)	A+
CompTIA	Security +
CompTIA	Network+
International Information Systems Security Certifications Consortium ((ISC)2)	Certified Information Systems Security Professional (CISSP)
(ISC)2	System Security Certified Practitioner (SSCP)
Information Systems Audit and Control Association (ISACA)	Certified Information Security Manager (CISM)
ISACA	Certified Information Security Auditor (CISA)
SecurityCertified.Net	Security Certified Network Professional (SCNP)
SecurityCertified.Net	Security Certified Network Architect (SCNA)
SANS Institute	GIAC Security Essentials Certification (GSEC)
SANS Institute	GIAC Security Leadership Certificate (GSLC)
SANS Institute	GIAC Security Expert (GSE)
SANS Institute	GIAC Information Security Fundamentals (GISF)

APPENDIX 4

AP4. SAMPLE STATEMENT OF ACCEPTANCE OF RESPONSIBILITIES

<IS NAME>

INFORMATION SYSTEM PRIVILEGED ACCESS AGREEMENT AND ACKNOWLEDGEMENT OF RESPONSIBILITIES

Date: _____

1. I understand there are two DoD Information Systems (IS), classified (SIPRNET) and unclassified (NIPRNET), and that I have the necessary clearance for privileged access to <IS NAME> [specify which IS the privileges are for]. I will not introduce or process data or software for the IS that I have not been specifically authorized to handle.

2. I understand the need to protect all passwords and other authenticators at the highest level of data they secure. I will not share any password(s), account(s), or other authenticators with other coworkers or other personnel not authorized to access the < IS NAME>. As a privileged user, I understand the need to protect the root password and/or authenticators at the highest level of data it secures. I will NOT share the root password and/or authenticators with coworkers who are not authorized <IS NAME > access.

3. I understand that I am responsible for all actions taken under my account(s), root or otherwise. I will not attempt to "hack" the network or any connected information systems, or gain access to data to which I do not have authorized access.

4. I understand my responsibility to appropriately protect and label all output generated under my account (including printed materials, magnetic tapes, floppy disks, and downloaded hard disk files).

5. I will immediately report any indication of computer network intrusion, unexplained degradation or interruption of network services, or the actual or possible compromise of data or file access controls to the appropriate <IS NAME > Information Assurance (IA) Management or senior IAT Level representatives. I will NOT install, modify, or remove any hardware or software (e.g., freeware/shareware, security tools) without written permission and approval from the <IS NAME > IAM or senior IAT Level representatives.

6. I will not install any unauthorized software (e.g., games, entertainment software) or hardware (e.g., sniffers).

7. I will not add/remove any users' names to the Domain Admins, Local Administrator or Power Users group without the prior approval and direction of the <IS NAME > IAM/or senior IAT Level representatives.

8. I will not introduce any unauthorized code, Trojan horse programs, malicious code, or viruses into the <IS NAME > local area networks.

9. I understand that I am prohibited from the following while browsing the web:

a. Introducing Classified and/or Unclassified Controlled Information (UCI) into a NIPRNet environment.

b. Accessing, storing, processing, displaying, distributing, transmitting, or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, or racist; that promotes hate crimes, or is subversive or objectionable by nature, including material encouraging criminal activity, or violation of local, State, Federal, national, or international law.

c. Storing, accessing, processing, or distributing Classified, Proprietary, UCI,, For Official Use Only (FOUO) or Privacy Act protected information in violation of established security and information release policies.

d. Obtaining, installing, copying, pasting, transferring, or using software or other materials obtained in violation of the appropriate vendor's patent, copyright, trade secret, or license agreement.

e. Knowingly writing, coding, compiling, storing, transmitting, or transferring malicious software code, to include viruses, logic bombs, worms, and macro viruses.

f. Promoting partisan political activity.

g. Disseminating materials unrelated to an established command religious program.

h. Using the system for personal financial gain such as advertising or solicitation of services or sale of personal property (e.g., eBay), or stock trading (i.e., issuing buy, hold and/or sell directions to an online broker).

i. Fundraising activities, either for profit or non-profit, unless the activity is specifically approved by the organization (e.g., organization social event fund raisers, charitable fund raisers, without approval).

j. Gambling, wagering, or placing of any bets.

k. Writing, forwarding, or participating in chain letters.

l. Posting personal home pages.

10. Personal encryption of electronic communications is strictly prohibited and can result in the immediate termination of access.

11. I understand that if I am in doubt as to any of my roles or responsibilities I will contact the <IS NAME > IAT Level III Supervisor for clarification.

12. I understand that all information processed on the <IS NAME> is subject to monitoring. This includes email and browsing the web .

13. I will not allow any user who is not cleared access to the network or any other connected system without prior approval or specific guidance from the <IS NAME > IAM.

14. I will use the special access or privileges granted to me ONLY to perform authorized tasks or mission related functions.

15. I will not use any <DoD/Component > owned information systems to violate software copyright by making illegal copies of software.

16. I will ONLY use my PRIVILEGED USER account for official administrative actions. This account will NOT be used for day-to-day network communications.

17. I understand that failure to comply with the above requirements will be reported and may result in the following actions:

a. Chain of command revocation of IS privileged access
b. Counseling
c. Adverse actions under the Uniform Code of Military Justice and/or criminal prosecution
d. Discharge or loss of employment
e. Revocation of Security Clearance

18. I will obtain and maintain required certification(s), according to DoD 8570.1-M and the certification provider, to retain privileged system access.

YOUR IAT Level III Supervisor is _____

INFORMATION SYSTEM NAME _____

IAT's NAME_____

IAT's SIGNATURE_____

Date_____

IA MANAGER LEVEL I NAME _____

IA MANAGER LEVEL I SIGNATURE _____

Date_____

(Level I or II Managers with privileged access will have signatures of the IA Manager Level II or III responsible for their IS functions).