



Defense Information Systems Agency
Department of Defense

**Defense Information Systems Agency
Information Assurance (IA) Workforce
Improvement Implementation Plan**

Prepared for

Defense Information Systems Agency
Chief Information Officer
5600 Columbia Pike
Falls Church, VA 22041-2770



DEFENSE INFORMATION SYSTEMS AGENCY

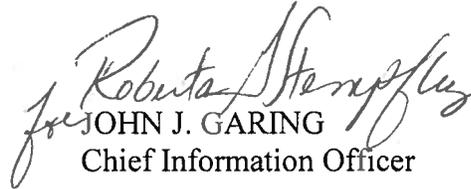
P.O. Box 4502
ARLINGTON, VIRGINIA 22204-4502

FOREWORD

This implementation plan is issued under the authority contained in DISAI 630-230-19 "Information Assurance," March 2, 2007 section 9.1. It provides guidance and procedures for the identification, training, certification, and management of the DISA workforce conducting Information Assurance (IA) functions in designated duty positions. It also provides information and guidance on reporting metrics and the implementation schedule.

This plan applies to DISA and to organizations and individuals contracted to perform DISA Information Technology (IT) outsourced based services or IT functions with DISA owned data or services.

This implementation plan is effective immediately.


JOHN J. GARING
Chief Information Officer

Summary of Changes

Revision No	Change Description
1	Corrected the title for the Director, Procurement/Chief, Defense Information Technology Contracting Organization (PLD/DITCO).
1	Changed PLD/DITCO responsibilities identified in section 3.3 to align with the responsibilities as defined in DISAI 610-225-2, 16 October 2007.
1	Removed references to the DISA IA Manual.
1	Clarified IAO term in relation to IAM (Overview paragraph 1.3)
1	Added table 5-1 which lists DoD baseline certifications.
1	Reworded section 6.1.4 to explain process of identifying IA workforce. Not all 2210 positions perform IA functions. The numerous data calls also identified other series that do perform IA functions.
1	Changed experience requirement in Appendix B tables (IAT I and IAM I) to read "1 to 4 years" and "1 to 5 years" respectively.
1	Changed the term "skill" to "requirement" in all tables identifying System Administrator (SA) attributes in Appendix C.
1	Added "IA designated" to the beginning of the first sentence and replaced "encourage" with "required" in section 5.2.3.
1	Added "Mandatory" to the label Annual IA Awareness Training, section 6.2.1.
1	Spelled out the acronym IAT in section 5.1.2.
1	Reworded section 6.3 to clarify IA training and certification funding sources and responsibilities.
1	Reworded section 5.1.3 to cover the situation where individuals who already possess higher level DoD approved certifications are fulfilling a lower level IA position.
1	Reworded Appendix E to comply with DoD/DISA guidance.
1	Replaced bullets with a numbering scheme throughout the document.
1	Reworded section 3.2.5 to more accurately reflect MPS role in the IA workforce.
1	Reworded section 5.2.1 to comply with current DISA Certification and Licensing Policy.
1	Reworded section 5.2.2 to comply with current DISA Certification and Licensing Policy. DISA will only pay for successful completion of exam.
1	Added section 5.2.6 to reflect ASD (NII)/DoD CIO decision to pay maintenance fees for certifications sponsored by ISC2 and ISACA.
1	Added tables 5-1, 5-2, 5-3 showing certification training modules available in DISA eLearning.
1	Removed previous sections addressing the implementation of an aggressive goal to certify workforce one year early. DISA will follow DOD guidelines of certifying workforce by end of CY 2010.
1	Removed "monitor" from second sentence in section 6.1.3.
1	Added Appendix B, definitions.
2	Removed references to MPS5 memo Professional Certification, Licensing, and Education Incentives, dated 23 April 2007 in the plan and removed MPS5 memo Professional Certification, Licensing, and Education Incentives, dated 23 April 2007 as a reference in Appendix A.
2	Updated section 5.2 to reflect DISA policy to pay for a maximum of two

Revision No	Change Description
	attempts to pass required certification test.
2	Updated section 6.4 to reflect final DoD ruling on contractor/contract compliance with 8570 requirements.

Table of Contents

1	Overview	1
2	Objectives	2
3	Roles and Responsibilities.....	3
3.1	Director for Strategic Planning and Information (SPI)/Chief Information Officer (CIO)	3
3.2	Director for Manpower, Personnel and Security (MPS)	3
3.3	Director, Procurement/Chief, Defense Information Technology Contracting Organization (DITCO)	4
3.4	Principal Directors of Strategic Business Units, Directors and Chiefs of Shared Services Units, Directors of Program Executive Offices, Direct Reports, and Special Advisors, Headquarters, DISA, and Commanders of DISA Combatant Command Field Offices4	
4	Key Implementation Actions and Milestones	6
4.1	PHASE 1 – Years 2006/2007 (Planning)	6
4.2	PHASE 2 - Year 2008 (Train and Certify)	8
4.3	PHASE 3 - Year 2009 (Train & Certify).....	8
4.4	PHASE 4 - Year 2010 (Train & Certify).....	9
5	Certification Policy, Process and Goals	10
5.1	IA Certifications	10
5.2	Certification Policy.....	11
5.3	Certification Process.....	14
5.4	Certification Goals.....	15
6	Implementation Requirements.....	17
6.1	IA Workforce Structure	17
6.2	IA Training	18
6.3	Budget.....	19
6.4	Contract (Contractor) Revisions	20
	APPENDIX A References.....	21
	APPENDIX B Definitions.....	22
	APPENDIX C DISA IA Training and Certification Program.....	26
	APPENDIX D DISA SA Training & Certification Program	35
	APPENDIX E DISA Statement of Information System Use And Acknowledgement of User Responsibilities	40

1 Overview

1.1. In accordance with provisions set forth in DoDD 8570.01, “Information Assurance Training, Certification, and Workforce Management”, of August 15, 2004, certified current as of April 23, 2007, DoD 8570.01-M, “Information Assurance Workforce Improvement Program”, December 19, 2005, and based on the responsibilities defined in DISA Instruction 630-230-19, “Information Assurance Policy”, March 2, 2007, this plan provides guidance for the identification and categorization of positions and certification of personnel conducting Information assurance (IA) functions within the DISA workforce supporting the DoD Global Information Grid (GIG).

1.2. As prescribed in DoDD 8570.01, all positions performing information system management or privileged access IA functions by category and level described in Chapters 3, 4, and 5 of DoD 8570.01-M will be identified. This applies to all positions with IA duties, whether performed as primary or additional/embedded duties. This requirement applies to all agencies military and civilian positions including those staffed by Local Nationals (LN), and to contractors if made part of the contract.

1.3. DoD IA policy has identified two initial IA categories, Information Assurance Technical (IAT) and Information Assurance Manager (IAM). These categories and levels are function based. Personnel performing the functions identified in DoD 8570.01-M tables C3.T3, C3.T5, C3.T7, C4.T3, C4.T5, or C4.T7 will be part of the IA workforce. In DoD 8570.01-M contents the term IAM includes the occupational titles of ISSO, IAO, ISSM, and TASO. It is anticipated in the near future additional IA categories will be identified and added to the IA workforce. This plan will address those additional categories when they are added to the DoD 8570.01-M.

2 Objectives

2.1. This plan prescribes the processes and procedures for the training, certification, and management requirements for the IA workforce as described in DoD 8570.01-M. These processes and procedures will allow for the development of a 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 information, information systems, and networks. This plan strives to:

2.1.1. Develop an 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 information, information systems, and networks.

2.1.2. Establish baseline technical and management IA skills among personnel performing IA functions.

2.1.3. Provide qualified IA personnel in each category and level.

2.1.4. 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.

2.1.5. Verify IA workforce knowledge and skills through standard certification testing.

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

3 Roles and Responsibilities

3.1 Director for Strategic Planning and Information (SPI)/Chief Information Officer (CIO)

Pursuant to the responsibilities prescribed in section 9.1 of DISAI 630-203-19, 2 March 2007, the Director SPI/CIO will have overall responsibility for the management of the implementation plan and will designate the Senior Information Assurance Officer, as the lead for this implementation process. SI3 will provide technical support and advisory services and closely coordinate the implementation activities with the relevant Directorates and Organizations across the Agency. SI3 specific responsibilities include:

3.1.1. Conducting initial IA orientation and annual awareness training in accordance with DoDD 8570.01.

3.1.2. Coordinating with MPS (training) to ensure sources of education and training are available for the IA workforce.

3.1.3. Coordinating with MPS to identify a system to track IA certifications in accordance with the requirements of DoD 8570.01-M.

3.1.4. Leading the submission of workforce improvement program (WIP) quantitative and qualitative reports in accordance with DoD 8570.01-M.

3.1.5. Coordinating with MPS in developing an IA training plan.

3.2 Director for Manpower, Personnel and Security (MPS)

In accordance with sections 9.4.4, 9.4.5, and 9.4.6 of DISAI 630-230-19, 2 March 2007, the Director MPS will ensure DISA IA requirements and responsibilities are incorporated into DISA personnel processes, support DISA training and certification of the IA workforce, and provide centralized tracking of DISA IA training and certification of the DISA IA workforce within the Agency. In support of implementing DoDD 8570.01 and DoD 8570.01-M requirements across the Agency, MPS specific responsibilities include the following:

3.2.1. Identifying the IA workforce (civilian, military, and contractor personnel) in accordance with DoD 8570.01-M.

3.2.2. Identifying all positions/personnel and entering the appropriate parenthetical title for both primary and/or additional duty responsibilities in the civilian personnel database in accordance with reference DoDD 8570.01.

3.2.3. Entering “INFOSEC” as the “Position Specialty Code” in the civilian personnel database for all positions/personnel performing IA functions in accordance with DoDD 8570.01.

3.2.4. Modifying all civilian position descriptions and military billet descriptions to reflect the training and certification requirements of DoD 8570.01-M.

3.2.5. Providing IA training for civilian and military personnel who are performing IA functions in IA designated positions and tracking their progress toward completing specific IA training requirements designated as prerequisites for IA certification examinations.

3.2.6. Providing necessary data for metrics and implementation status reports in accordance with DoD 8570.01-M.

3.3 Director for Procurement/DITCO(PLD), Defense Information Technology Contracting Organization

In accordance with section 10.12 of DISAI 610-225-2, 16 October 2007, the Director PLD/DITCO serves as the principal advisor and functional authority to the Director, DISA, for procurement activities. The Director, PLD/Chief, DITCO, will:

3.3.1. Provide functional expertise in the development and promulgation of policies, plans, and procedures for procurement and contract administration.

3.3.2 Provide direct procurement support to programs, projects, and services.

3.3.3 Provide DISA-wide subject matter expertise in the areas of procurement.

3.3.4 When the appropriate DFAR/FAR regulations have been approved and implemented, coordinate and work with requirements officials to assist in the inclusion of proper contractual language regarding DoD 8570.01-M IA contract and contractor requirements.

3.3.5 Provide necessary information support to SI34/35 in fulfilling annual FIMSA and DoD IA qualitative and quantitative data reports.

3.4 Principal Directors of Strategic Business Units, Directors and Chiefs of Shared Services Units, Directors of Program Executive Offices, Direct Reports, and Special Advisors, Headquarters, DISA, and Commanders of DISA Combatant Command Field Offices

In accordance with sections 9.7.1 and 9.7.6 of DISAI 630-230-19, 2 March 2007, these individuals will ensure all IT systems and programs under their supervision are planned, funded, tested, implemented, monitored, and executed in a manner consistent with DoD and DISA IA plans, policies, and requirements and designate appropriate government and

contractor personnel to be part of the IA Workforce, and ensure all personnel, including contractors, successfully complete IA awareness training and certification commensurate with their respective responsibilities. In support of implementing DoDD 8570.01 and DoD 8570.01-M requirements across the Agency, their specific responsibilities include:

3.4.1. Ensuring IA workforce personnel comply with the training and certification requirements prescribed in DoD 8570.01-M.

3.4.2. Supporting the DISA IA implementation requirements of DoDD 8570.01 and DoD 8570.01-M.

3.4.3. Supporting the processes and procedures outlined in this memorandum.

3.4.4. Developing IA workforce budget plans for training and certification.

3.4.5. Ensuring DoDD 8570.01 and DoD 8570.01-M requirements are included in all contracts requiring IT services.

3.4.6. Providing necessary data for metrics and required implementation status reports.

4 Key Implementation Actions and Milestones

In order to achieve the objectives identified in section 2 the following activities are required:

4.1 PHASE 1 – Years 2006/2007 (Planning)

Objective	Office of Primary Responsibility (OPR)	Summary Milestones	Scheduled Completion Date	Status
Establish governance structure and process	CIO	Develop DISA IA Working Group	Mar 2006	Completed.
	CIO/MPS	Identify DISA IA workforce	Mar 2007	Completed.
	MPS/CIO	Develop a methodology to identify IA workforce	Nov 2006	Completed Nov 2006 (MPS 43 modified JTD to incorporate IA data tags.
	CIO	Develop a DISA IA Policy	Oct 2006	Completed Dec 2006.
	MPS/CIO	Develop a DISA training plan	Nov 2007	Completed. Part of implementation plan.
	MPS/CIO	Develop a plan to track IA training and certifications	Dec 2007	Completed. LMS is the tool of choice, manual process is backup.
	Identify DISA IA workforce	MPS/CIO	Initiate data calls	Oct 2006
	MPS/CIO/DIR IAMs	Identify IA billets and personnel required to perform IA functions	Dec 2007	Ongoing. (Using results of data call completed in Oct 2006 as a baseline. Will execute quarterly updates to refine IA workforce and billets.).
	MPS/CIO/DIR IAMs	Identify contractors in IA positions	Dec 2007	Ongoing. Capturing contractor data during data calls. No automated means exists to track data; everything is manual.
	Requirement Offices	Ensure contractor personnel possess necessary IA certification		* On hold (waiting for AUSD/AT&L resolution)

Objective	Office of Primary Responsibility (OPR)	Summary Milestones	Scheduled Completion Date	Status
	MPS/SPI	Capability to track contractor certification and status		* On hold (waiting for AUSD/AT&L resolution)
	Requirement Offices	Modify existing contracts to reflect DOD 8570.01-M requirements		* On hold (waiting for AUSD/AT&L resolution)
	Requirement Offices	Ensure future contracts reflect DOD 8570.01-M requirements for contractors		* On hold (waiting for AUSD/AT&L resolution)
	COR/TMs	Ensure contractor IA certifications are reflected in DEERS		* On hold (waiting for AUSD/AT&L resolution)
	COR/TMs	Ensure CORS understand their requirement to enter required data into a DMDC applications that feeds into DEERS		* On hold (waiting for AUSD/AT&L resolution)
Certification Training and Testing	MPS	Provide initial IA certification training and testing requirements	Sep 2007	Completed
User IA Awareness Policy	MPS/CIO	Provide for initial IA orientation and training	Jun 2006	Completed
	MPS/CIO	Provide for annual IA awareness training	Mar 2007	Completed
Budget	All Directorates	Develop a budget plan to support implementation and sustainment of IA workforce requirements	Dec 2007	Ongoing

ACCOMPLISHMENT: 10% certified

** Until the Defense Federal Acquisition Regulations are modified to reflect the DoD 8570.01-M requirements for IA contracts and contractor personnel, DISA is focusing on its civilian and military IA workforce.*

4.2 PHASE 2 - Year 2008 (Train and Certify)

Objective	OPR	Summary Milestones	Scheduled Completion Date	Status
	MPS	Develop training plan for phase 2	Feb 2008	
	MPS	Upgrade training for next 30% IA workforce members based on lessons learned	Mar 2008	
	MPS/CIO	Arrange and conduct next 30% IA workforce certifications	May 2008	
	CIO	Conduct annual IA Awareness training	Jun 2008	
	CFE	Milestone Budget Plan	Jul 2008	

GOAL: 40% certified

4.3 PHASE 3 - Year 2009 (Train & Certify)

Objective	OPR	Summary Milestones	Scheduled Completion Date	Status
	MPS	Develop training plan for phase 3.	Jan 2009	
	MPS	Upgrade training for next 30% IA workforce members based on lessons learned	Mar 2009	
	MPS/CIO	Arrange and conduct next 30% IA workforce certifications	May 2009	
	CIO	Conduct annual IA Awareness training	Jun 2009	
	CFE	Milestone Budget Plan	Jul 2009	

GOAL: 70% certified

4.4 PHASE 4 - Year 2010 (Train & Certify)

Objective	OPR	Summary Milestones	Scheduled Completion Date	Status
	MPS	Develop training plan for phase 4.	Jan 2010	
	MPS	Upgrade training for next IA workforce members based on lessons learned	Mar 2010	
	MPS/CIO	Arrange and conduct next IA workforce certifications	May 2010	
	CIO	Conduct annual IA Awareness training	Jun 2010	
	CFE	Milestone Budget Plan	Jul 2010	

GOAL: 100% certified

5 Certification Policy, Process and Goals

5.1 IA Certifications

5.1.1. DISA will accept any of the certifications listed in the following table for each category and level. A certification can apply to more than one level. An individual only needs one of the “approved certifications” for his or her IA category and level to meet the minimum requirement.

IAT Level I	IAT Level II	IAT Level III
A+	GSEC	CISA
Network+	Security+	CISSP
SSCP	SCNP	GSE
	SSCP	SCNA
IAM Level I	IAM Level II	IAM Level III
GISF	CISM	CISM
GSLC	GSLC	GSLC
Security+	CISSP	CISSP

Table 5-1 DoD Approved Baseline Certifications

5.1.2. Information Assurance Technical (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:

5.1.2.1. The A+ or Network+ certification qualify only for IAT Level I and could not be used for IAT Level II positions.

5.1.2.2. The SSCP certification qualifies for both IAT Level I and IAT 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.

5.1.3. As prescribed in DoD 8570.01-M, management certifications corresponding to the position level do not cascade down. Each position requires an individual to meet one of the specific certifications associated with that management level. For example, personnel fulfilling an IA designated position as an IAM level I only needs to complete one of the three certifications listed in table 5-1 for that category and level. This case is the norm and covers the majority of management level certification situations. However, in the event an individual is fulfilling a IAM Level I position who already has a CISSP, CISM, or GSLC certification; DISA will not require them to obtain one of the DoD approved

IAM level I certifications. This situation is considered outside the norm and is intended to cover new hires or individuals who already have higher level DoD approved certifications.

5.1.4. IATs must also obtain certifications required to implement the IA requirements for their specific operating system environment (e.g., Microsoft Operating Systems Administrator Certification, Unix Systems Administrator, etc.), unless the operating system certification is included in one of the approved DoD IA Certifications. DISA will use successful completion of a formal class in the environment operating system to meet this requirement. Successful completion means passing the end of course examination with a score of 80 percent or better.

5.1.5. Situations where employees fail to pass the certification examination will be handled on a case by case basis and could result in the employee being reassigned to a position without IA responsibilities per DoD 8570.01-M.

5.1.6. DISA personnel (i.e., civilian or military) who are in designated IA positions performing IA functions on December 31, 2007 have until the end of calendar year 2010 to complete their required certifications. Any employee assuming new IA duties after the effective date of this implementation plan will be required to obtain certification within 6 months of assuming these new IA duties. Supervisors and organizational level IAMs are responsible for tracking and monitoring the certification progress of their employees.

5.1.7. Situations where employees fail to obtain and/or maintain the necessary certifications will be handled on a case by case basis and could result in the employee being reassigned to a position without IA responsibilities per DoD 8570.01-M.

5.2 Certification Policy

5.2.1. The DISA IA Workforce Improvement Implementation Plan establishes a baseline of validated (tested) knowledge that is relevant, recognized, and accepted across the Department of Defense. The following provides guidance on the DISA certification policy as it applies to the DISA IA workforce.

5.2.1.1. Payment and reimbursement will be subject to availability of funds.

5.2.1.2. Since IA certification is a new requirement, DISA will pay for a maximum of two attempts for passing a DoD approved IA certification examination. If an employee fails on the first attempt, their Directorate IAM and Supervisor will assist in developing a remediation strategy for re-testing. Although the strategy will be tailored for each individual, at a minimum it will involve re-taking review classes (concentrating on examination weak areas) and scoring a minimum of 85% on certification pre-tests. Once the remediation requirements are successfully met and verified by their supervisor and Directorate IAM, the individual can schedule their second attempt. Situations where employees fail to pass the certification examination after the allowed number of

attempts or fail to maintain their certified status will be handled on a case by case basis and could result in the employee being reassigned to a position without IA responsibilities per DoD 8570.01-M.

5.2.1.3. DISA will pay for license/certification fees (initial, renewal, and registration).

5.2.1.4. DISA will not pay for association membership fees required in obtaining or maintaining a license or certification. [DoD DIAP will fund IA association membership fees for CY 2008].

5.2.2. There are different methods available to the IA work force for payment of certification examination costs. A qualified employee can pay for their own costs and seek re-imburement, or a qualified employee can use a voucher purchased by DISA, in which case the procedures are as follows:

5.2.2.1 Organizational Level IAM and employee Supervisor will verify the employee is working in an IA position and is thoroughly prepared to test.

5.2.2.2 If the employee fails the examination they must complete the remediation requirements stated in section 5.2.1.2. Once the remediation requirements are successfully met and verified by their supervisor and Directorate IAM, the individual can schedule their next attempt.

5.2.3. In order to prepare for certification, civilian and military employee's direct supervisors will provide an IA Development Plan. The development plan will identify the employee's IA category and level and their certification and training requirements for their IA position. The plan will also address the various types of training available to meet their IA certification and training requirements. For instance, the DISA eLearning - Computer Based Training (CBT) site has numerous training courses available that will assist in preparing individuals in meeting professional certification requirements. Tables 5-2 and 5-3 are examples of the modules available on DISA eLearning for CompTIA and ISC2 sponsored certifications. The DISA eLearning site also offers mentoring services and practice examinations for these vendor sponsored certifications.

Certified Information Systems Security Professional (CISSP)		
Title	Number	Hours
Information Security and Risk Management	243962 ENG	3.00
Security Architecture and Design	243975 ENG	2.50
Access Control	243986 ENG	2.50
Application Security	243998 ENG	2.00
Operations Security	244020 ENG	2.50
Cryptography	244031 ENG	2.00
Physical (Environmental) Security	244059 ENG	2.00
Telecommunications and Network Security	244069 ENG	3.50
Business Continuity and Disaster Recovery Planning	244085 ENG	2.50

Business Continuity and Disaster Recovery Planning	244085 ENG	2.50
Legal, Regulations, Compliance and Investigations	244096 ENG	2.50
Systems Security Certified Practitioner (SSCP)		
Title	Number	Hours
Access Controls	206534 ENG	1.75
Administration	206535 ENG	2.75
Auditing and Monitoring	206536 ENG	2.25
Risk, Response, and Recovery	206537 ENG	2.25
Cryptography	206538 ENG	2.5
Data Communications	206539 ENG	2.25
Malicious Code	206540 ENG	1.25

Table 5-2 ISC2 Certification Training Modules on DISA e-Learning

CompTIA A+ 2006 Essentials		
Title	Number	Hours
Personal Computer Component	242525 ENG	2.75
Laptop Components, Peripherals, and Networks	242526 ENG	3.25
Operating Systems	242527 ENG	2.50
Security, Safety, and Communication	242528 ENG	2.00
CompTIA A+ 2006 IT Technician		
Title	Number	Hours
Installing, Configuring, and Troubleshooting PC Components	245875 ENG	2.00
Working with Laptops and Portable Devices	245876 ENG	1.25
Understanding and Maintaining Networks	245877 ENG	2.50
Maintaining Operating Systems	245878 ENG	3.00
Installing and Troubleshooting Printers and Scanners	245879 ENG	1.50
Managing IT Security	245880 ENG	1.50
Recognizing Safety Procedures, Effective Communication, and Professional Behavior	245881 ENG	1.25
CompTIA Network+ 2005		
Title	Number	Hours
The Fundamentals of Networking	218678 ENG	3.50
LAN Technologies	218693 ENG	3.50
Networking Protocols	218703 ENG	2.50
IP Addressing and Sub netting	218741 ENG	2.75
Working with TCP/IP	221224 ENG	1.75
WANs and Remote Connectivity	218759 ENG	2.25
Network Operating Systems and Clients	218763 ENG	2.00
Network Security	218760 ENG	2.75
Network Troubleshooting	218761 ENG	2.75
Fault Tolerance and Disaster Recovery	218762 ENG	1.75
CompTIA Security+		
Title	Number	Hours

General Security Concepts	84869 ENG	6.00
Communications Security	84870 ENG	6.00
Infrastructure Security	84871 ENG	7.00
Encryption Technologies	65873 ENG	5.00
Operational and Organizational Security	84873 ENG	6.00

Table 5-3 CompTIA Certification Training Modules on DISA e-Learning

5.2.4. In addition to the DISA eLearning on-line training, there are other training sessions available for DoD employees on a web site sponsored by Carnegie Mellon. The Carnegie Mellon web site is called the Virtual Training Environment (VTE) and is located at <https://www.vte.cert.org>. It offers on-line training sessions as well as pre-certification practice examinations. MPS51 also offers formal training courses quarterly throughout the year. Supervisors need to be aware of the time requirements required for individuals to become trained and certified.

5.3 Certification Process

5.3.1 The IA workforce certification process is prescribed in the following steps.

Step 1. Employee is serving under a permanent appointment in an IA designated position.

Step 2. Employee and Supervisor/Organization Level IAM agree on which certification based on the employee's IA position. They also agree on a timeframe to complete the certification (current employees fulfilling an IA designated position have until end of CY 2010, new employees or hires have 6-months from the date of hire or appointment).

Step 3. Employee and Supervisor agree on a training methodology (web based training, self study, or formal classroom) to include taking and passing pre-certification tests with at least a score of 80 percent or better. Pre-certification tests are available on the DISA eLearning and Carnegie Melon VTE web sites.

Step 4. The Supervisor and Organization Level IAM track employee's progress. This will be a manual process until DISA has an automated tool.

Step 5. Employee completes training and pre-tests requirements. Employee presents supporting documentation to Supervisor and Organization Level IAM. Organization Level IAM or Supervisor notifies MPS51, employee is eligible for one of the methods described above in section 5.2.2 for payment of examination costs.

Step 6. Employee takes and passes certification examination. Once employee completes the DISA specific IA training prescribed in Appendix C, then the employee is a trained member of the IA workforce.

5.3.2. If an employee fails to pass the certification examination, their Organizational Level IAM and Supervisor will assist in developing a remediation strategy for re-testing. Although the strategy will be tailored for each individual, at a minimum it will involve re-taking review classes, DISA eLearning modules, or other web-based training (concentrating on examination weak areas) and scoring a minimum of 85% on certification pre-tests. Once the remediation requirements are successfully met and verified by their Supervisor and Organizational Level IAM, the individual can schedule their next attempt. Situations where employees continue to fail the certification examination or fail to maintain their certified status will be handled on a case by case basis and could result in the employee being reassigned to a position without IA responsibilities per DoD 8570.01-M.

5.3.3. Assistant Secretary of Defense for Networks Information and Integration /DoD Chief Information Officer (ASD (NII)/DoD CIO) will pay for the CY 2008 certification maintenance fees required by International Information Systems Security Certifications Consortium (ISC2) for CISSP and SSCP and by the Information Systems Audit and Control Association (ISACA) for CISSM and CISA for DoD (civilian and military) certified individuals.

5.3.4. DISA has established a training program to ensure personnel assigned to enhance and protect DISA's information technology environments are effectively trained to administer and secure these environments. Training can be acquired through formal classroom or by on-the-job working experience. The program provides the DISA specific training required in support of the minimum industry certifications listed in the DoD 8570.01-M. Program oversight will be accomplished by the Information Assurance Support Branch (SI35). MPS51 will provide training management support. IA Managers will monitor IA certification training and maintain records of IA certifications and OJT. The DISA IA training program is described in Appendix C and the DISA SA training program is described in Appendix D.

5.4 Certification Goals

5.4.1. To allow for the proper identification and planning of the IA requirements, DoD has adopted a phased implementation approach. The base years (CY 2006/2007) provide time for the identification of specific requirements to support budget and staffing planning, and to certify the initial 10 percent of the IA workforce. DoD requires 30 percent workforce compliance for the next three years (CY 2008, CY 2009, and CY 2010) with full compliance at the end of calendar year 2010.

5.4.2. In order to achieve this goal, Directors, Program Managers, and Supervisors will encourage their employees in IA designated positions to complete the IA certification and training requirements as soon as they are ready. Directors, Program Managers, and Supervisors will discuss and set IA training and certification goals for their employees in IA designated positions as part of their annual Individual Development Plan (IDP) process review. They should use this time to emphasize to their IA workforce employees the benefits of completing the training and certification requirements as soon as possible

as opposed to waiting. These benefits include career advancement opportunities and participating in training and certification courses while funding is available.

6 Implementation Requirements

The following requirements listed in Chapter 9 of DoD 8570.01-M, December 19, 2005 is further clarified for DISA implementation.

6.1 IA Workforce Structure

6.1.1. **Designated Accrediting Authority (DAA)** - “Requirements” (Chapter 5, DoD 8570.01-M). Director for Strategic Planning and Information (SPI) /Chief Information Officer (CIO) as the DAA for the Agency, and the Vice Director for Strategic Planning and Information (SPI)/Chief Information Officer (CIO), as the alternate DAA, must be certified in accordance with the provisions set forth in DoD 8570.01-M.

6.1.2. **Privileged Access Positions** - “Identify positions performing privileged access IA functions” DoD 8570.01-M (C1.4.4.4) and “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” DoD 8570.01-M (C2.1.4); a sample is shown in Appendix D. Directors, Program Managers, and Supervisors will ensure that their technical category personnel maintain those certifications and requirements necessary to be authorized unsupervised privilege access to systems. Supervisors will maintain copies of the signed privileged access agreement.

6.1.3. **Track Position Certifications** - “Identify, track, and monitor IA personnel performing IA functions to ensure IA positions are staffed with trained and certified personnel.” DoD 8570.01-M (C1.4.4.7). MPS51 with assistance from SI35 will identify and track IA personnel. IAMS and supervisors will monitor the training and certification of IA personnel performing IA functions. The DISA Learning Management System (LMS) will be used to assign and track certification goals for the DISA IA Workforce (civilian and military). Until the LMS is fielded an alternative manual process will be used. MPS51 will ensure courses are available to support the certification requirements. MPS51 will manage and track reimbursement processes.

6.1.4. **Identification and Recording of Defense Civilian Personnel Data System (DCPDS) Parenthetical Titling** - “Identify all GS-2210 positions/personnel using the Office of Personnel Management specified parenthetical titles per OPM Job Classification Standard. 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.” DoD 8570.01-M (C1.4.4.10). “Enter “INFOSEC” as the “Position Specialty Code” into DCPDS per DoDD 8570.01 for all positions/personnel performing IA functions as primary, additional, or embedded duty and their category and level.” DoD 8570.01-M (C1.4.4.11). MPS43 has identified and tagged all DISA GS-2210 positions in

the Joint Table of Distribution. This information was used to initially identify the IA positions/personnel across the agency through several data calls. During the data calls, the list was scrubbed to exclude 2210 series that were not performing IA functions and identify other job series that were performing IA functions. The results of the data calls have been recorded and positions performing IA functions have been tagged and labeled accordingly. MPS1 and MPS2 will coordinate the revision of the Position Descriptions (PD) and Military billet descriptions to reflect IA certification and training requirements for the DISA designated IA positions as specified in DoD 8570.01-M.

6.1.5. Failure to Certify - “Individuals in IA positions 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.” DoD 8570.01-M (C2.3.4). DISA will certify their IA workforce as prescribed in DoD 8570.01-M and will aggressively pursue full compliance as expeditiously as possible. However, given the current quantity of “certified” IA personnel in the organization and possible funding constraints, DISA will follow the waiver process identified in sections DoD 8570.01-M C3.2.4.2, C3.2.4.3, C4.2.3.2.1, or C4.2.3.4.2 as necessary. Employees who fail to meet the certification or waiver requirement will not be able to perform IA related functions. **Personnel who fail to certify and have privilege access will have that access removed.** MPS1 will review the employee’s qualifications and possibilities for reassignment to other vacant positions within the Agency.

6.1.6. Incremental Changes - “Plan for, and incrementally complete these requirements over four years from the effective date of DoD 8570.01-M.” (IA WIPAC modified base year to calendar year 2007). (C9.2.1.1). If funds are available and personnel are ready to take the certification exams, then they should not wait 4 years to certify. Directors, Program Managers, and supervisors must consider the operational needs of their organizations as well when approving personnel for training to certify since a key objective of certification is to keep our IA workforce current in technology used to assure our information systems. As part of the annual IDP review, requirements for obtaining IA certification will be discussed with employees and training/certification requirements and goals outlined. MPS51 will adjust training resources as necessary to support certification of IA personnel performing IA functions. Since certification is a DoD requirement for IA personnel (government civilian and military), they must be provided time to take certification examinations during official duty time.

6.2 IA Training

6.2.1. Mandatory Annual IA Awareness Training - “Collect metrics and submit reports to ASD (NII)/DoD CIO to support planning and analysis of the IA workforce and annual FISMA reporting.” DoD 8570.01-M (C1.4.4.3, C1.4.4.8, Chapter 6). SI34/35 conducts this annual requirement, collects metrics for the status across the Agency and reports the status in the FISMA annual report.

6.2.2. **Authorized User Minimum IA Orientation and Awareness** - “Requirements.” (Chapter 6 DoD 8570.01-M). DISA personnel will use the DoD IA Awareness online or Computer Based Training as the baseline standard. These training products can be accessed by the IASE web site. Additional DISA specific awareness training may be required by MPS Security and/or SI35.

6.2.3. **Recertifications** - “Completion of sustainment training/continuing education as necessary to maintain certification status.” DoD 8570.01-M (C3.2.3.3). As stated in section 5.2.1.3 of this plan, DISA will pay for fees associated with maintaining the employee’s (civilian and military) certification status.

6.3 Budget

6.3.1. DISA must report progress on budgeting necessary for implementing IA certification within the directed 4-year period in accordance with DoD 8570.01-M (C9.4). Table 6-3 is an example of the format for this report.

6.3.2. Funding is for DoD personnel (civilian and military) only. DISA will not pay for certification of contractors.

6.3.3. Although the Assistant Secretary of Defense for Networks and Information Integration Department of Defense Chief Information Office (ASD(NII)/DoD CIO has provided the initial funding for training and certification costs through the implementation phase, the amount does not cover all the necessary costs. MPS51 training has been covering the additional costs; however, Principal Directors of Strategic Business Units, Directors and Chiefs of Shared Services Units, Directors of Program Executive Offices, Direct Reports, and Special Advisors, Headquarters, DISA, and Commanders of DISA Combatant Command Field Offices need to be prepared to provide funding assistance should any shortfall training funding requirements occur during the implementation phase and need to plan for training and certification costs in the out-years (CY 2011 and beyond).

6.3.4. Principal Directors of Strategic Business Units, Directors and Chiefs of Shared Services Units, Directors of Program Executive Offices, Direct Reports, and Special Advisors, Headquarters, DISA, and Commanders of DISA Combatant Command Field Offices need to provide the necessary budget information in order for SI3 to report progress on budgeting to meet IA training and certification costs as required by DoD 8570.01-M.

IA Workforce Milestone Budget Plans (Training and Certification Costs)							
IA WF Budget	PY 2007	CY 2008	BY 2009	BY 2010	BY 2011	BY 2012	BY 2013
Required							
Budgeted							

IA Workforce Milestone Budget Plans (Training and Certification Costs)							
Obligated							

Table 6-3 IA Workforce Milestone Budget Plans

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

6.4 Contract (Contractor) Revisions

6.4.1 DOD 8570.01-M states the IA training and certification requirements apply to contractors and contracts providing support DoD information systems. DoD has issued a final rule amending the Defense Federal Acquisition Regulation Supplement (DFARS) to address training requirements that apply to contractor personnel who perform information assurance functions for DoD. Contractor personnel accessing information systems must meet applicable training and certification requirements. This ruling has an effective date of January 10, 2008.

APPENDIX A References

DISA Instruction (DISAI) 630-230-19, "Information Assurance Policy", 2 March 2007

DISA Instruction (DISAI) 610-225-2, "Acquisition Oversight and Management", 16 October 2007

DoD 8570.01-M, "Information Assurance Workforce Implementation Program", 19 December 2005

DoD Instruction (DoDI) 8500.2, "Information Assurance Implementation", 6 February 2003

DoD Directive (DoDD) 8500.01E, "Information Assurance", 24 October 2002, Certified Current as of 23 April 2007

DoD Directive (DoDD) 8570.01, "Information Assurance Training, Certification, and Workforce Management", 15 August 2004, Certified Current as of 23 April 2007

Office of Management and Budget Circular A-130, "Management of Federal Information Resources, Transmittal 4", 30 November 2000, Appendix 3

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

Section 3544 of Title 44, United States Code (as added by the Federal Information Security Management Act (FISMA) of 2002)

APPENDIX B Definitions

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.

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

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 of DoD 8570.01-M.

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.

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 DoD 8570.01-M, 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.

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.

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

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.

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.

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.

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

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, of June 2006.

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

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.

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

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.

Duty.

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.

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 responsibilities. The position would normally require 15 to 24 hours, out of a 40(+) hour week, devoted to IA functions.

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.

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.

Enclave. Collection of Computing Environment (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 Office of Management and Budget (OMB A-130 (Reference (i)) dtd April 2000. 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.

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

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)).

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.

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.

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.

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.

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 information systems and networks. The IA workforce includes anyone with privileged access and IA managers who perform any of the responsibilities or functions described in DoD 8570.01-M. In the near future, 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.

Local National (LN). 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.

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.

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:

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

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

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

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

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.

IA Training Program.

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

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

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

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

APPENDIX C DISA IA Training and Certification Program

- References:**
- (a) Department of Defense (DoD) Directive 8570.01, “Information Assurance Training, Certification, and Workforce Management”, certified current as of 23 April 2007
 - (b) Department of Defense (DoD) Manual 8570.01-M, “Information Assurance Workforce Improvement Program”, 19 December 2005
 - (c) Department of Defense (DoD) Directive 8500.01E, “Information Assurance”, certified current as of 23 April 2007
 - (d) Department of Defense (DoD) Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003

Discussion

Reference (a) establishes policy and assigns responsibilities for the Department of Defense (DoD) Information Assurance (IA) training, certification, and workforce management.

Reference (b) provides guidance and procedures for training, certification, and management of the DoD workforce conducting Information Assurance (IA) functions in assigned duty positions. The IA workforce includes but is not limited to all individuals performing the IA functions as described in the reference manual.

Reference (c) establishes the policy and assigns the responsibilities under title 10 to achieve Department of Defense (DoD) Information Assurance (IA) through a defense in depth approach that integrates the capabilities of personnel, operations, and technology, and supports the evolution of network centric warfare.

Reference (d) implements the policy, assigns responsibilities, and prescribes procedures for applying integrated, layered protection of the DoD information systems and networks.

Notes: Training and certification requirements for personnel performing specialized IA functions including system architecture and engineering, computer network defense, certification and accreditation, and vulnerability assessments are forthcoming.

Although IAT functions are very similar to SA functions, current DISA guidance is the SA positions will not be replaced by IAT positions. Both IAT and SA positions will be staffed.

Personnel fulfilling IAT designated positions must be certified as a DISA SA Level I prior to certification as an IAT.

IAT functional requirements are cumulative. Thus an IAT Level II or Level III requires mastery of the functional requirements of the preceding levels.

IAM functional requirements are not cumulative; however, in the event a person is fulfilling an IAM level I who already has a higher level DOD

approved certification such as a CISSP, GSLC, or CISM; they will not be required to obtain one of the IAM level I DoD approved certifications.

In accordance with references (a) and (b) and in support of references (c) through (d), the DISA IA training and certification program is as follows.

Program

Level I Requirements

Information Assurance Technical (IAT) Level I

IAT Level I personnel make the Computing Environment (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 the following table.

IAT Level I	
Attribute	Requirement
Experience	Normally has one to four years of experience in IA technology or a related field.
System Environment	Computing 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.

The training and certifications requirements are:

IAT Level I Training and Certification Requirements
IA Hot Subjects (latest version)
UNIX Security for System Administrators (latest version)*
Windows 2000 Security (Windows CE)*
VMS online training (System Administration)**
Information Assurance Policy & Technology (IAP&T) (latest version)***
Firewall and Router Fundamentals (latest version)***
PKI (latest version)***
Plus approved certifications****
Complete core skill checklist

* Note: Either UNIX Security for System Administrators or Windows 2000 Security (Windows CE) is required, not both.

** Either on-line or classroom training.

*** If not previously completed for DISA SA Level I.

**** The approved certifications are:

- A+
- Network+
- SSCP+

Submit completed Level I core skills checklist, training, and certification documentation to organizational IAM.

Upon successful completion of the training material, certification test, and core skills checklist, the individual will be certified as an IAT Level I.

Information Assurance Management (IAM) Level I

IAM Level I personnel are responsible for the implementation and operation of a DoD Information System (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 the following table.

IAM Level I	
Attribute	Requirement
Experience	Usually an entry level management position with one 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).

The training and certification requirements are:

IAM Level I Training and Certification Requirements
Information Assurance for Professionals Shorts (latest version)
SSAA Preparation Guide (latest version)
Information Assurance Policy & Technology (IAP&T) (latest version)*
PKI (Latest version)*
Firewall and Router Fundamentals (latest version)*
VMS online training (ISSM Module)*
DoD IT Portfolio Repository (DITPR) training
Approved certification**
Complete core skills checklist

* If not previously completed

**The approved certifications are:

- GISF
- GSLC
- Security+

Submit completed Level I core skills checklist, training, and certification documentation to organizational IAM.

Upon successful completion of the training material, certification test, and core skills checklist, the individual will be certified as an IAM Level I.

Level II Requirements

Information Assurance Technical (IAT) Level II

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 the following table.

IAT Level II	
Attribute	Requirement
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.

The training and certification requirements are:

IAT Level II Training and Certification Requirements
Windows Server 2003 Incident Preparation & Response (IP&R): Part I (latest version)*
System Administrator Incident Preparation & Response for UNIX (SAIPR UNIX) (latest version)*
Approved certification**
Complete core skills checklist

*Either UNIX Security for System Administrators or Windows 2000 Security (Windows CE) is required, not both.

** The approved certifications are:

- GSEC
- SCNP
- Security+
- SSCP

Submit completed core skills checklist, training and certification documentation to organizational IAM.

Upon successful completion of the training material, certification test, and core skills checklist, the individual will be certified as an IAT Level II.

Information Assurance Management (IAM) Level II

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 the following table.

IAM Level II	
Attribute	Requirement
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.

IAM Level II	
Attribute	Requirement
Other	Relies on experience and judgment to plan and accomplish goals. Manages IA operations for an NE(s).

The training requirements are:

IAM Level II Training Requirements
Information Assurance for Professionals Shorts (latest version)
SSAA Preparation Guide (latest version)
Introduction to the DoD Information Technology Security Certification & Accreditation Process (DITSCAP) (latest version)
Information Assurance Policy & Technology (IAP&T) (latest version)*
PKI (latest version)*
Firewall and Router Fundamentals (latest version)*
VMS online training (ISSM Module)*
DoD IT Portfolio Repository (DITPR) training
Approved certification**
Complete core skill checklist

* If not previously completed

**The approved certifications are:

- GSLC
- CISM
- CISSP

Submit completed core skills checklist, training, and certification documentation to organizational IAM.

Upon successful completion of the training material, certification test, and core skills checklist, the individual will be certified as an IAM Level II.

Level III Requirements

Information Assurance Technical (IAT) Level III

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 the following table.

IAT Level III	
Attribute	Requirement
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.

There are no DISA training requirements identified at this time.

The approved certifications are:

- CISA
- GSE
- CISSP
- SCNA

Submit completed core skills checklist and certification documentation to organizational IAM.

Upon successful completion of the certification test and core skills checklist the individual will be certified as an IAT Level III.

Information Assurance Management (IAM) Level III

IAM Level III personnel are responsible for ensuring all enclave information systems 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 the following table.

IAM Level III	
Attribute	Requirement
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).

If an IAM Level III previously completed any of the following training requirements, then they do not need to retake that particular training. The following table lists the level III requirements.

IAM Level III Training Requirements
Information Assurance for Professionals Shorts (latest version)
SSAA Preparation Guide (latest version)
Introduction to the DoD Information Technology Security Certification & Accreditation Process (DITSCAP) (latest version)
Information Assurance Policy & Technology (IAP&T) (latest version)
PKI (latest version)
Firewall and Router Fundamentals (latest version)
VMS online training (ISSM Module)
DoD IT Portfolio Repository (DITPR) training
Approved certification
Complete core skill checklist

The approved certifications are:

- CISM

- GSLC
- CISSP

Submit completed core skills checklist and certification documentation to organizational IAM.

Upon successful completion of the certification test and core skills checklist, the individual will be certified as an IAM Level III.

Recertification

IA professionals will comply with the recertification requirements of their specific approved certification. IA professionals are required to maintain their certification status while fulfilling IA designated positions.

APPENDIX D DISA SA Training & Certification Program

- References:**
- (a) Committee on National Security Systems (CNSS) Instruction 4013, “National Information Assurance Training Standard for System Administrators (SA)”, March 2004
 - (b) Department of Defense (DoD) Directive 8570.01, “Information Assurance Training, Certification, and Workforce Management”, Certified Current as of 23 April 2007
 - (c) Department of Defense (DoD) Instruction 8500.2, “Information Assurance (IA) Implementation”, 6 February 2003
 - (d) Chairman of the Joint Chiefs of Staff Manual (CJCSM) 6510.01, “Defense in Depth: Information Assurance (IA) and Computer Network Defense (CND)”, 25 March 2003

Discussion

A System Administrator (SA), as defined in reference (b), is an individual responsible for the installation and maintenance of an Information System (IS), providing effective IS utilization, adequate security parameters, and sound implementation of established Information Security (INFOSEC) policy and procedures. Reference (a) states the SA works closely with Information Systems Security Officers and Managers (IAOs and IAMs per reference (c)) to ensure the IS or network is operated securely.

Reference (d) states certification programs for SAs should include the following subject areas: configuration control; installation; operations and maintenance; user account management; system selection; access control; response, recovery, and/or reconstitution; incident response; operations monitoring and analysis; and countermeasures. The reference further states **ALL** SAs will be certified and cleared to the level of information classification of a given system.

In support of the guidance and requirements prescribed in references (a) through (d), the DISA SA training and certification program is as follows.

Notes:

At a minimum, all DISA SAs must be certified as SA Level I.

SA Level I certification is required prior to unsupervised root access.

JTF/GNO CTO 2006-02 requires PKI training for all DISA SAs

Training will include:

PKI Awareness Training

How to configure systems for CAC/PKI logon

How to configure systems for DIGITAL SIGNATURE

How to configure systems for EMAIL ENCRYPTION

How to configure systems for WEBSERVER SOFT CERTIFICATES Program

Level I Requirements

A Level I SA or Entry Level SA is relatively inexperienced and is considered a trainee. The typical level I SAs environment is generally a small localized local area network (LAN) with few users and no additional servers other than the domain controller. Until certified, Entry Level SAs must operate under the supervision of a DISA certified SA. The general skill sets are:

SA Level I	
Attribute	Requirement
Experience	At least one year administrating the relevant operating system.
Formal training	Operating system and command language or network protocols/operating parameters (network administration).
Knowledge	Rudimentary system/network administrator tasks relevant to the operating system or network. Normal operating parameters of relevant systems and applications.
Other	Strong customer relation skills.
	Listed in PLS with contact information.
	Dot mil Email addresses (xxxx.xxx@xxx.mil).

The training and certification requirements are:

SA Level I Training and Certification Requirements
DOD Information Assurance Awareness, (latest version)
Information Assurance Policy & Technology (IAP&T), (latest version)
Firewall and Router Fundamentals, (Latest Version)
PKI online training (until a DoD standard course is available, either AF or Navy course)
VMS online training (System Administration module)
If required HBSS SA training
Complete core skills checklist
Pass certification test (80% or higher)

Submit completed core skills checklist, training, and certification test documentation to the organizational IAM. The organizational IAM will submit all documentation to MPS51 (Training).

Upon successful completion of the training material, certification test, and core skills checklist, the individual will be certified as a DISA Level I SA.

Level II Requirements

A Level II SA is more experienced and has greater responsibilities. Their environment typically consists of larger networks with multiple domains, several types of servers, and a larger user population. They are the workhorses of a domain, who perform the majority of the daily tasks that keep a domain running smoothly. They are efficient in multitasking; able to work several problems simultaneously. At least one Level II SA must be assigned in organizations operating large mission-critical networks with multiple domains, several types of serves, and large user populations. A Level II SA must exhibit mastery of all Level I SA requirements. The general skill sets are:

SA Level II	
Attribute	Requirement
Experience	At least 3 years experience in administrating the relevant operating system.
Formal Training	Networking, programming language concepts and algorithms, firewall management and telecommunication fundamentals.
Knowledge	Interactions within their domain.
Other	Ability to program in a command language Ability to spot and automate redundant tasks.
	Strong communications skills. Can explain solutions for complex problems to users and other system administrators.
	Independently solving non-trivial problems.
	Assist IAO/IAM in implementing security mechanisms on networks and systems within their domain.
	Listed in PLS with contact information.
	Dot mil Email addresses (xxxx.xxx@xxx.mil).

The training and certification requirements are:

SA Level II Training and Certification Requirements
Windows Server 2003 Incident Preparation & Response (IP&R): Part I (latest version)*
System Administrator Incident Preparation & Response for UNIX (SAIPR UNIX) (latest version)*
Introduction to the DoD Information Technology Security Certification & Accreditation Process (DITSCAP) (latest version)
Complete core skill checklist
Pass certification test with (80% or higher)

* Either UNIX or Windows Operating System, is required not both.

NOTE: INCLUDE ELearning

Level II SA certification test is the exam given at the end of the formal operating system course arranged by MPS51 (Training).

Complete Level II SA core skills checklist and submit to organizational IAM. The organizational IAM will submit all documentation to MPS51 (Training).

Upon successful completion of the training material, certification test, and core skills checklist, the individual will be certified as a DISA Level II SA.

Level III

Level III SAs are highly experienced and are generally in the higher military grades (officers, warrant officers, senior enlisted) or civilian equivalent. They are responsible for managing resources, policy, and/or supervising other SAs. Level III SAs must demonstrate mastery of Level I SA and Level II SA requirements.

Level III SAs are responsible for ensuring all enclave information systems are functional and secure. They support, monitor, test, and troubleshoot hardware and software IA problems pertaining to the CE, NE, and enclave environments. They determine the enclaves long term IA system needs and acquisition requirements to accomplish operational objectives. They also develop and implement information security standards and procedures through the certification and accreditation process.

DISA Level III SA certification is restricted to government civilian/military personnel only.

SA Level III	
Attribute	Requirement
Experience	At least 7 to 10 years of experience in management and administering the relevant operating system.
Formal Training	Data/Algorithm Structure, Machine Architecture, Networking, Programming Language Concepts/Algorithms.
Knowledge	A strategic view of the domain operation/mission, and interaction with all external domains.
	Extensive knowledge of a variety of IA field's concepts, practices, and procedures to ensure the secure integration and operation of all enclave systems.
Other	Fluency in at least one command language. Knows applicable programming languages and security vulnerabilities of those languages.
	Strong communications skills. Can explain solutions for complex problems to users and other system administrators.
	Ability to work independently to quickly and completely solve problems.
	In depth knowledge of local and DoD security and IA policies.
	Listed in PLS with contact information.
	Dot mil Email addresses (xxxx.xxx@xxx.mil).

Level III SA training and certification requirements are:

Must be certified Level II SA in two operating systems.

Must have experience managing large enclaves.

Must have the skills and abilities to manage and direct the technical efforts of the Level II SA and Level I SAs under his or her direct supervision.

Must have completed formal technical and security training in a number of core computer science courses to include network and network security and possess a good understanding of the capabilities/vulnerabilities of the operating systems he or she manages.

In addition to satisfying the coursework requirements for Level I SA and Level II SA, the Level III SA must be proficient in operating system design and machine architecture.

Complete Level III SA core skills checklist and submit to organizational IAM. The organizational IAM will submit all documentation to MPS51 (Training).

Upon successful completion of the training material and core skills checklist, the individual will be certified as a DISA Level III SA.

Recertification

SAs are required to be recertified every 18 months. They will recertify at their current level of certification. They will be required to complete all the training and certifications requirements for recertification.

APPENDIX E DISA Statement of Information System Use And Acknowledgement of User Responsibilities

NAME: _____
(Last name, first – print)

Date: _____

Type of Access: Authorized___ Privileged___ Both___

FOR AUTHORIZED ACCESS:

I will use DISA information systems for authorized purposes only. I will not introduce or process data for which the Information System has not been specifically authorized to handle. I understand that all information processed on DISA controlled information systems are subject to monitoring. This includes Email and web browsing. I may also be held both criminally and financially responsible for any damages that may occur to the network, systems, other electrical and non-electrical equipment or computing devices, if my actions are determined to be deliberate, willful, or malicious.

I understand the need to protect all passwords at the highest level of data they secure. I will not share my password(s) or account(s) information with other coworkers or other personnel not authorized to access the information system.

I understand that I am responsible for all actions taken under my account(s) either as an Authorized¹ or Privileged² user. I will not attempt to “hack” the network, any connected Information Systems, or gain access to data for which I am not authorized to access.

I understand my responsibility to appropriately protect and label all output generated under my account (to include printed materials, USB devices, floppy disks and downloaded hard disk files).

I understand I must have the requisite security clearance and documented authorization (by my supervisor) of my need-to-know before accessing DISA/DoD information and information systems.

I understand my responsibility to ensure Privacy Act, and other protected personal information (such as personally identifiable information) is protected while it is being, processed or accessed. In computer environments outside the DISA physical data processing installations requiring access to DISA information and information systems (such as remote job entry stations, terminal stations, minicomputers, microprocessors, and similar activities) I know I must ensure appropriate protection of personal and sensitive data.

In accordance with the DoD CIO memorandum on *Policy on Use of Department of Defense (DoD) Information Systems - Standard Consent Banner and User Agreement*,

November 2, 2007, I understand by signing this document I acknowledge and consent that when I access DISA and/or any DoD information system:

- I am accessing a U.S. Government information system (as defined in CNSSI 4009) that is provided for U.S. Government-authorized use only.
- I consent to the following conditions:
 - o The government routinely monitors communications occurring on this information system, and any device attached to this information system, for purposes including, but not limited to, penetration testing, communications security (COMSEC) monitoring, network defense, quality control, employee misconduct in investigations, law enforcement investigations, and counterintelligence investigations.
 - o At any time, the government may inspect and/or seize data stored on this information system and any device attached to this information system.
 - o Communications occurring on or data stored on this information system, or any device attached to this information system, are not private. They are subject to routine monitoring and searched.
 - o Any communications occurring on or data stored on this information system, or any device attached to this information system, may be disclosed or used for any U.S. Government-authorized purpose.
 - o Security protections may be utilized on this information system to protect certain interests that are important to the government. For example, passwords, access cards, encryption or biometric access controls provide security for the benefit of the government. These protections are not provided for your benefit or privacy and may be modified or eliminated at the government's discretion.

I understand that I am prohibited from the following:

- a. Introducing classified information into an unclassified system or environment.
- b. Accessing, storing, processing, displaying, distributing, transmitting or viewing material that is abusive, harassing, defamatory, vulgar, pornographic, profane, racist, promotes hate crimes, or subversive in nature, or objectionable by nature to include; material that encourages criminal activity, or violate any applicable local, state, federal, national or international law.

c. Violating the established security, release, and protection policies for information identified as Classified, Proprietary, Unclassified Controlled Information, For Official

Use Only (FOUO), or Privacy Act during the information handling states of storage, process, distribution or transmittal of such information

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. This includes peer-to-peer file sharing software or games.

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 activities.

g. Disseminating religious materials outside 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. Engaging in fund raising activities, either for profit or non-profit unless the activity is specifically approved by the command (e.g., Command social event fund raisers, charitable fund raisers, etc., without approval).

j. Gambling, wagering or placing of any bets.

k. Writing, forwarding or participating in chain letters.

l. Posting personal web pages, using my personally-owned information technology (IT such as personal electronic devices [PEDs], personal data assistants [PDAs], laptops, thumb drives etc.), or non-DISA controlled information technology on DISA controlled computing assets.

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

FOR THOSE WITH PRIVILEGED ACCESS:

In addition to satisfying all of the responsibilities of an Authorized User, as a Privileged user, I understand the need to protect the root or super user password at the highest level of data it secures. I will **NOT** share the super user or root password with co-workers who are not authorized access.

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 Information Assurance (IA) Management or Senior IA Technical Level representatives. I will **NOT** install, modify, or remove any

hardware or software (e.g. freeware/shareware, security tools, etc.) without written permission and approval from the IA Management or senior IA Technical Level representative. I will **NOT** remove or destroy system audit, security, event or any other logs without prior approval from IA Management or senior IA Technical Level representative.

I will only use my PRIVILEGED USER account for official administrative actions. This account is **NOT** to be used for day-to-day network communications, unless explicitly approved.

I understand that if I am in doubt as to any of my roles or responsibilities I will contact the Senior IA Management or Senior IA Technical Level representative for clarification.

I will **NOT** install any unauthorized software (e.g. games, entertainment software, etc) or hardware (e.g. sniffers).

I will **NOT** add any user names to the Domain Admins, Local Administrator or Power Users group without the prior approval and direction of the IA Management/or Senior IA Technical Level representative.

I will **NOT** introduce any unauthorized code, Trojan horse programs, malicious code or viruses into DISA information systems or networks.

I will **NOT** allow any user access to the network or any other connected system that is not cleared without prior approval or specific guidance of the IA Management or Senior IA Technical Level representative.

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

I will **NOT** use any DISA controlled information systems to violate software copyright by making illegal copies of software.

ALL MUST READ AND SIGN:

I understand that failure to comply with the requirements of this User Agreement will be reported and investigated. The results of the investigation may result in one or all of the following actions:

- a. Immediate revocation of system access and/or user privileges
- b. Job counseling, admonishment
- c. Uniform Code of Military Justice and/or criminal prosecution
- d. Reassignment, discharge, or loss of employment

I HAVE READ, UNDERSTOOD, AND WILL COMPLY WITH THE REQUIREMENTS SET FORTH IN THIS AGREEMENT.

NAME: _____ (signed)

TITLE: _____

IA MANAGER LEVEL I NAME _____

(printed)

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

IA MANAGER LEVEL I SIGNATURE _____

Date _____