MILITARY HEALTH SYSTEM (MHS) **INFORMATION ASSURANCE (IA) IMPLEMENTATION GUIDE**	**IMPLEMENTATION GUIDE No. 13**	
	EFFECTIVE DATE **07/19/05**	**REVISED DATE** **05/20/10**

Subject:

INFORMATION ASSURANCE TRAINING, EDUCATION, AND AWARENESS

1. PURPOSE AND SCOPE

1.1. The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

2. POLICY

2.1. It is MHS policy that:

2.1.1. TMA shall develop an IA workforce with a common understanding of the concepts, principles, and applications necessary to enhance protection and availability of the TMA network.

2.1.2. All TMA users shall receive initial IA awareness orientation as a condition of network access.

3. PROCEDURES

3.1. Military Health System (MHS) Chief Information Officer (CIO) shall:

3.1.1. Ensure compliance with roles and responsibilities stated in Department of Defense (DoD) 8570.01-M, “Information Assurance Workforce Improvement Program,” December 19, 2005 with Change 2, April 20, 2010.

3.1.2. Provide appropriate representation on the Information Assurance Training, Certification, and Workforce Management Oversight Advisory Council.

3.1.3. Ensure managers are trained on processes required to support the IA workforce improvement program.

3.2. MHS Office of the Chief Information Officer/Information Assurance (OCIO/IA) shall:

3.2.1. Collect TMA IA workforce metrics and submit an annual report to the Assistant Secretary of Defense (Networks and Information Integration) ASD(NII).

3.2.2. Ensure IA personnel who do not meet certification or training requirements, or have allowed certifications to expire, are not permitted privileged access.

3.2.3. Consolidate information for the IA Workforce Implementation Milestone Budget for IA training, certification, and workforce management from data submitted by TMA Components.

3.3. TMA Office of Administration shall:

3.3.1. Ensure the appropriate background investigation is obtained before unsupervised privileged access or management responsibility is granted to any TMA system.

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

3.3.3. Ensure that TMA personnel, identified as part of the IA workforce, are trained and certified in ASD(NII)/DoD CIO-approved certifications outlined in DoD 8570.01-M. (Appendices 2 and 3).

3.3.4. Identify all General Schedule (GS)-2210 positions/personnel using Office of Personnel Management (OPM) or National Security Personnel System (NSPS) specified terminology.

3.4. TMA Network Operations Director shall:

3.4.1. Provide initial IA orientation to all TMA employees and contractors.

3.4.2. Provide annual awareness training to all TMA employees and contractors.

3.4.3. Ensure all TMA employees and contractors complete both initial and annual IA training.

3.5. TMA Directorates shall:

3.5.1. Identify civilian, military, and contractor positions and personnel performing IA functions and whether those functions are primary, additional, or embedded.

3.5.1.1. Primary – A position with primary duties focused on IA functions. Although a primary position may have other duties assigned, the main effort would normally require at least 25 to 40(+) hours per week devoted to IA functions.

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

3.5.1.3. 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.

3.5.2. Assign civilian and military positions with IA responsibilities to the IA Technical and IA Management categories and further assign levels I-III to each position based on guidance provided in DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, Incorporating Change 2, April 20, 2010.

3.5.3. Identify IA functions performed by contractors and ensure all contracts reflect these training and certification requirements.

3.5.4. Identify all contractor positions performing IA functions, designate them as either IA Technical or IA Management, and further assign positions to levels I-III within each category based on guidance provided in DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, Incorporating Change 2, April 20, 2010.

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

3.5.6. Modify pre-existing contracts to specify these training and certification requirements.

3.5.7. Develop budget data and provide to OCIO/IA for consolidation into the IA workforce reporting requirements.

3.5.8. Provide the OCIO/IA with all information necessary for completing the annual report.

3.6. Director, TMA Procurement Support Division shall:

3.6.1. Ensure contractor certification and training requirements are specified in all contracts for the acquisition of IA services.

3.6.2. Ensure contractor personnel supporting IA functions are appropriately certified prior to executing a contract.

3.6.3. Ensure the IA certification category and level of contractors performing IA functions are documented in the Defense Enrollment Eligibility Reporting System (DEERS).

3.7. TMA Designated Accrediting Authorities (DAAs) shall:

3.7.1. Complete DAA certification within sixty days of assignment to the position.

3.7.1.1. Certification may be obtained either from the Defense Information Systems Agency's (DISA) computer-based training (CBT) or Web-based training located on the DoD IA Portal or through the National Defense University's Information Resources Management College.

3.7.1.2. Sign the DAA CBT certificate upon completion of the CBT course and obtain the signature of the Chief, Career Development Branch.

3.7.1.3. The signed certificate is to be filed in the training record.

3.7.2. Maintain the course completion certificate, as a part of their official personnel files.

3.7.3. Recertify every three years.

4. REFERENCES

1. DoDD 8570.01, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004, Certified Current as of April 23, 2007
2. DoD 8570.01-M, "Information Assurance Workforce Improvement Program," December 19, 2005, Incorporating Change 2, April 20, 2010

5. ACRONYMS

ASD(NII) .....Assistant Secretary of Defense (Networks and Information Integration)
CBT.....Computer-Based Training
CIO .....Chief Information Officer
DAA.....Designated Accrediting Authority
DEERS.....Defense Enrollment Eligibility Reporting System
DISA .....Defense Information Systems Agency
DoD.....Department of Defense
DoDD.....Department of Defense Directive
DoDI .....Department of Defense Instruction
GS .....General Schedule
IA .....Information Assurance
ISC 2 .....International Information Security Certification Consortium
JMIS.....Joint Medical Information Systems
MHS.....Military Health System

NSPS.....National Security Personnel System
OPM.....Office of Personnel Management
OTJ .....On-the-job
PEO.....Program Executive Office
TMA .....TRICARE Management Activity
TRO .....TRICARE Regional Office

Appendix 1
Information Assurance Technical Category, I-III

DoD 8570.01-M, "Information Assurance Workforce Improvement Program,"
19 December, 2005, Incorporating Change 2, April 20, 2010

Civilian, Military, Contractor* IA Technical (IAT) Level I to III (Foreign National (FN) Levels I & II only)	
Initial Training**	**Yes**
IA Certification (Appendix 3)	**Yes (within 6 months)**
OTJ Evaluation	**Yes (for initial position)**
Computing Environment 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 for the CISSP))**
Background Investigation	**As required by IA level**
Sign Privileged Access Statement	**Yes**
*Contractor category, level, and certification requirements to be specified in the contract **Classroom, Distributive, Blended, Government or Commercial Provider	

Appendix 2
Information Assurance Management (IAM) Category, I-III

DoD 8570.01-M, "Information Assurance Workforce Improvement Program,"
19 December, 2005, Incorporating Change 2, April 20, 2010

Civilian, Military, Contractor* IA Management (IAM) Level I to III (Foreign National (FN) Levels I & II only)	
Initial Training* **	**Yes**
IA Certification (Appendix 3)	**Yes (within 6 months)**
OTJ Evaluation	**No**
Computing Environment Certification	**No**
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 for CISSP))**
Background Investigation	**As required by IA level**
*Requirements to be stated in contract ***Classroom, Distributive, Blended or Commercial Provider	

Appendix 3

DoD 8570.01-M, "Information Assurance Workforce Improvement Program,"
19 December 2005, Incorporating Change 2, April 20, 2010

DoD IA Approved Baseline Certifications, including IAT & IAM "Cascade-Down" Details

IA Technical Level I		IA Technical Level II		IA Technical Level III
A+	GSE	GSEC	CISA	CISA
Network+	SCNA	Security+	CISSP	CISSP
SSCP	GSEC	SCNP	GSE	GSE
CISA	Security+	SSCP	SCNA	SCNA
CISSP	SCNP	GCIH		GCIH
GCIH				
IA Management Level I		**IA Management Level II**		**IA Management Level III**
GISF	CAP	GSLC	CAP	GSLC
GSLC	CISM	CISM		CISM
Security+	CISSP	CISSP		CISSP