



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

OCT 10 2008

MEMORANDUM FOR: TRICARE MANAGEMENT ACTIVITY
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL
INFORMATION SYSTEMS OFFICE
TRICARE REGIONAL OFFICE – NORTH
TRICARE REGIONAL OFFICE – SOUTH
TRICARE REGIONAL OFFICE – WEST

SUBJECT: Military Health System (MHS) Information Assurance (IA) Policy Guidance
and MHS IA Implementation Guides

In accordance with Assistant Secretary of Defense (Health Affairs) (ASD (HA)) memorandum, "Military Health System (MHS) Information Assurance (IA) Implementation Guides," dated July 19, 2005, this office has completed a review of the MHS IA Implementation Guides. As a result, the following documents have been updated:

- Implementation Guide No. 1, "Governance"
- Implementation Guide No. 2, "Sanitization"
- Implementation Guide No. 3, "Incident Reporting"
- Implementation Guide No. 4, "Employee Behavior"
- Implementation Guide No. 7, "Data Integrity"
- Implementation Guide No. 9, "Configuration Management"
- Implementation Guide No. 10, "System Life Cycle Management"
- Implementation Guide No. 11, "Public Key Infrastructure (PKI) and PK Enabling"
- Implementation Guide No. 12, "IAVM Program"
- Implementation Guide No. 13, "IA Training, Education and Awareness"
- Implementation Guide No. 14, "INFOCON"

The MHS IA Implementation Guides were developed in collaboration with the MHS IA Working Group, and staffed, coordinated, and approved by the Enterprise Architecture Board.

The provisions of the MHS IA Implementation Guides are policy for all TRICARE Management Activity (TMA) Directorates, TRICARE Regional Offices (TROs), and the Joint Medical Information Systems (JMIS) Office.

For TRICARE Contractors, these documents are policy if required by contract; otherwise, they serve as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate these documents into their information assurance policies and procedures.

For additional information, please contact Ms. Dorothy S. Williams, Chief, MHS IA Program at (703) 681-7735 or via e-mail at dorothy.williams@tma.osd.mil.



Charles M. Campbell
Chief Information Officer
Military Health System

Attachments:
As stated

cc:
Deputy Surgeon General of the Army
Deputy Surgeon General of the Navy
Deputy Surgeon General of the Air Force

 <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS)</p> <p style="text-align: center;">INFORMATION ASSURANCE (IA)</p> <p style="text-align: center;">IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 1	
	EFFECTIVE DATE 07/19/05	REVISED DATE 10/10/08
<p>Subject:</p> <p style="text-align: center;">GOVERNANCE</p>		

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.

1.2. The MHS Information Assurance (IA) program provides governance and oversight through the collaboration of the MHS Chief Information Officer (CIO), the MHS Office of the Chief Information Officer/Information Assurance, (OCIO/IA), the TMA Privacy Office, the JMISO, and the Service Medical Departments. The intent is to reaffirm the relationship between governing bodies and promote collaboration in order to enhance IA interoperability and to improve information system security practice efficiencies. Governance of the MHS IA program consists of those functions that contribute to the effective implementation of an MHS-wide IA program and is comprised of the following sub-program elements: program management, planning, budgeting, staffing (human resources), and performance measurement.

2. POLICY

2.1. It is MHS Policy that:

2.1.1. Develop and promulgate policies and procedures to ensure IA is integrated into the planning, procurement, development, implementation, and management of the MHS infrastructure and information systems (ISs) in accordance with DoDD 8500.01E, “Information Assurance (IA),” October 24, 2002, certified current as of April 23, 2007.

3. PROCEDURES

3.1. MHS Chief Information Officer shall:

3.1.1. Develop policy to ensure IA is integrated into all policies and procedures used to plan, procure, develop, implement, and manage the MHS infrastructure and ISs in accordance with DoDD 8500.01E, "Information Assurance (IA)," October 24, 2002, certified current as of April 23, 2007.

3.1.2. Define strategic IA goals and annual objectives through appropriate Information Management/Information Technology (IM/IT) documents, and ensure such goals and objectives are funded, achieved, and monitored.

3.1.3. Collect and report IA management, financial, and readiness data to meet DoD IA internal and external reporting requirements.

3.1.4. Recommend information classification, sensitivity, and need-to-know for MHS information and Mission Assurance Category (MAC) Levels for MHS Centrally Funded Systems to the Director, TMA, in accordance with DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003.

3.1.5. Ensure the MHS Designated Accrediting Authorities (DAAs) appointed by the Director, TMA, accredit each DoD IS in accordance with DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007.

3.1.6. Establish, resource, and implement IA training and certification programs for all TMA Component personnel in accordance with DoD Directive (DoDD) 8570.1, "Information Assurance Training, Certification, and Workforce Management," August 15, 2004 (Change 1).

3.1.7. Ensure that Public Key Infrastructure (PKI) implementation within MHS ISs complies with DoDI 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004.

3.1.8. Ensure IA is integrated into the MHS enterprise architecture.

3.2. MHS OCIO/IA shall:

3.2.1. Ensure the integrity, availability, confidentiality, non-repudiation and authentication of MHS information technology (IT) Information Systems (ISs).

3.2.2. Support military readiness and peacetime healthcare, Certify and Accredited (C&A) centrally managed systems, and communicate security related IT issues or items of interest affecting the DoD.

3.2.3. Test, verify and assure adequate security controls for information technology systems supporting the DoD in the accomplishment of its healthcare mission.

3.2.4. Establish, manage, and assess the effectiveness of the MHS IA Program.

3.2.5. Identify technical standards necessary to acquire, protect, manage, integrate, and secure information technology systems across the MHS environment.

3.2.6. Ensure Risk Assessments are accomplished for TRICARE Contractor ISs, TMA Director's ISs, and Centrally Managed Systems.

3.2.7. Budget for C&A security testing, to include travel, risk assessment, documentation review, hardware and software, and specific security training.

3.2.8. Ensure that performance measurements are established for the IA program and are consistent with the OCIO Performance Objective as reported in the Annual Performance Plan submittal.

3.2.9. Provide guidance for the IA component of the MHS enterprise architecture.

3.2.10. Provide guidance for security awareness, certification, education, and training.

3.2.11. Manage the Information Assurance Vulnerability Management (IAVM) program.

3.2.12. Chair the Information Assurance Working Group (IAWG).

3.2.13. Staff the IA function with individuals who, as a team, have the skill mix to manage, plan, budget, execute, and measure the performance of the IA program.

3.3. TMA Privacy Office shall:

3.3.1. Develop, implement, maintain, and oversee security requirements for electronic Protected Health Information (PHI).

3.3.2. Ensure that the requirements for electronic PHI are integrated into all policies and procedures for the planning, procurement, development, implementation, and management of the MHS infrastructure and information systems.

3.3.3. Provide guidance, direction, and oversight to ensure that internal audits of PHI access and use are performed. Ensure policies for internal controls enable the prevention and detection of significant instances or patterns of illegal, unethical, or improper conduct.

3.3.4. Ensure a response to alleged violations of rules, regulations, policies, procedures, and codes of conduct by evaluating or recommending the initiation of investigative procedures.

3.3.5. Provide guidance, direction, and oversight of workforce policies and procedures to ensure consistent action is taken for failure to comply with security policies for all employees on the workforce.

3.3.6. Ensure a formal incident reporting and response capability exists.

3.3.7. Receive reports of security breaches, coordinate appropriate action(s) to minimize harm, investigate breaches, and make recommendations to management for corrective action.

3.3.8. Administer the DoD 5200.2-R, "Personnel Security Program," January 1987 (Changes 1, 2, and 3) as required, issue guidance or interim authority to access DoD systems and coordinate letters of trustworthiness for Information Technology (IT)/Automated Data Processing (ADP) adjudication packages.

3.4. Joint Medical Information Systems Office shall:

3.4.1. Provide IA guidance, direction, and oversight to program managers under its purview to ensure IA requirements for ISs are implemented.

3.4.2. Budget for C&A security testing, to include travel, risk assessment, documentation review, hardware and software, specific security training, and formal incident reporting and response capability of TMA Centrally Managed Systems.

3.4.3. Monitor the IA programs and C&A results of the systems under its control, and provide feedback to the OCIO/IA as appropriate.

3.4.4. Collaborate with the OCIO/IA and the Service Medical Departments to develop OCIO/IA policy and guidance, and provide feedback regarding application of current OCIO/IA policy and guidance.

3.4.5. Staff the IA function with individuals who, as a team, have the skill mix to manage, plan, budget, execute, and measure the performance of the IA program.

3.5. Service Medical Departments, Chief Information Officers shall:

3.5.1. Distribute MHS IA guidance to military treatment facility Commanders.

3.5.2. Collaborate with the OCIO/IA and the JMISO to develop OCIO/IA policy and guidance, and provide feedback regarding application of current OCIO/IA policy and guidance.

3.5.3. Provide representation at meetings of the IA Working Group.

3.6. TRICARE Contractors shall:

3.6.1. Comply with contractual requirements regarding DoD C&A procedures, physical, and personnel security.

3.6.2. Ensure individual and organizational accountability for implementing the IAVM program and protecting ISs that access DoD ISs or data in accordance with contract language.

3.7. MHS Information Assurance Working Group (IAWG) (see **Figure 1**):

3.7.1. The IAWG shall serve as the primary conduit for information and policy guidance flow between the OCIO/IA, the TMA Components, and CIOs of the Service Medical Departments. The OCIO/IA shall ensure the IAWG provides a forum for issue identification, issue resolution, and corporate decision making. Service representatives to the IAWG are expected to keep their respective Service IA Program Managers and CIOs up to date on all IA issues addressed at the IAWG, as well as coordinate IA policy and procedure decisions. Members and attendees shall be encouraged to use the MHS IAWG as the conduit for promulgating issues, gathering comments/consensus points, and developing agenda items for meetings.

3.7.2. The IAWG ensures that the MHS CIO and the ASD(HA) are informed of all IA issues impacting the MHS. Any guidance or policy issued by the OCIO/IA that is staffed through the IAWG, shall be sent to either the MHS CIO or ASD(HA) for approval.

3.7.3. The IAWG also monitors and provides IA guidance for joint initiatives between the MHS and the Veterans Health Administration (VHA). The VHA is invited to participant in the IAWG meetings.

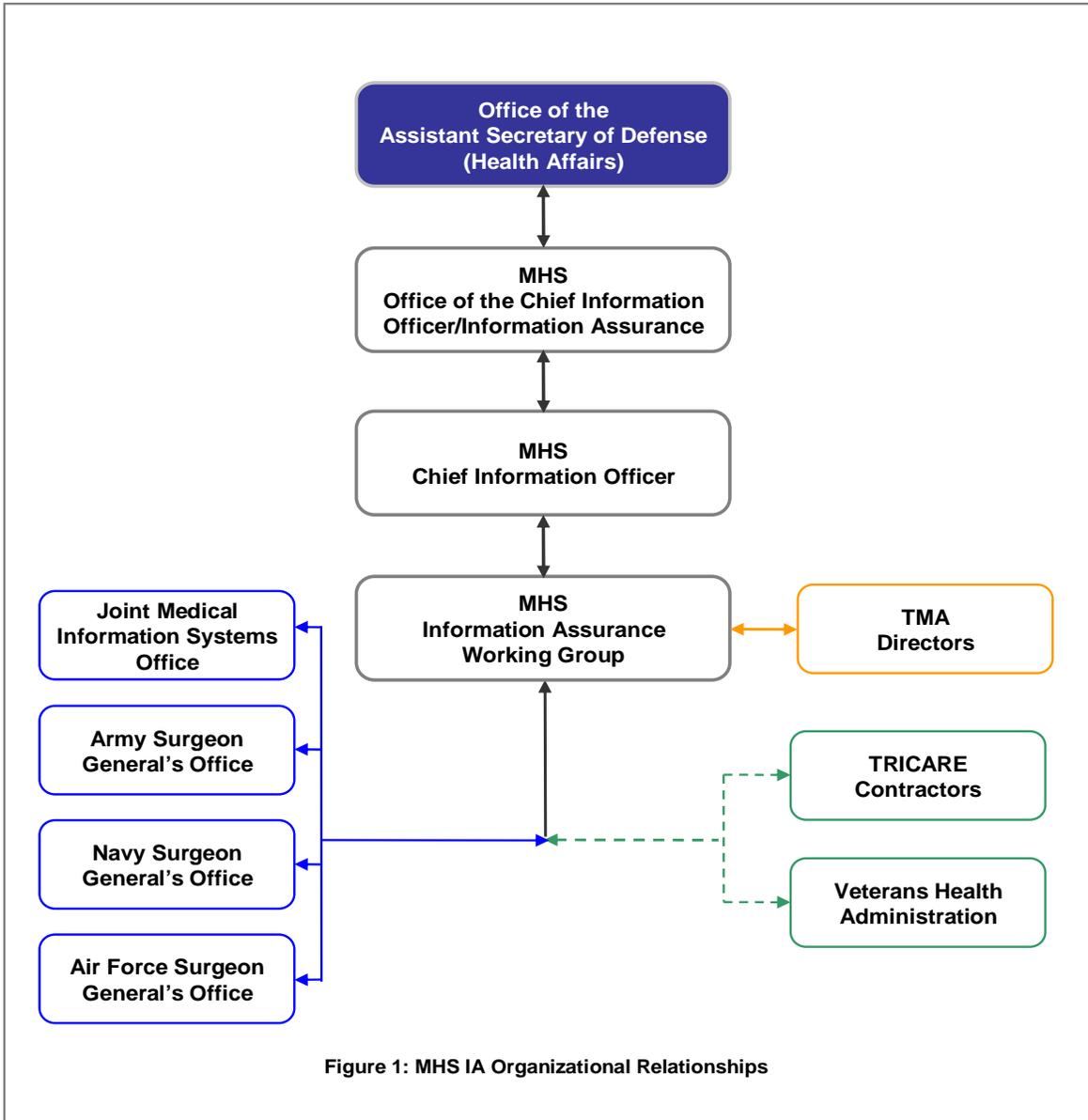


Figure 1: MHS IAWG Organization

4. REFERENCES

1. DoD 5200.2-R, "Personnel Security Program," January 1987 (Changes 1, 2, and 3)
2. DoDD 8500.01E, "Information Assurance (IA)," October 24, 2002, certified current as of April 23, 2007
3. DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003
4. DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007
5. DoDI 8520.2, "Public Key Infrastructure (PKI) and Public Key (PK) Enabling," April 1, 2004

6. DoDD 8570.1, “Information Assurance Training, Certification, and Workforce Management,” August 15, 2004 (Change 1)

5. ACRONYMS

ADP.....	Automated Data Processing
ASD(HA)	Assistant Secretary of Defense(Health Affairs)
C&A.....	Certification and Accreditation
CIO.....	Chief Information Officer
DAA.....	Designated Accrediting Authority
DIACAP.....	DoD Information Assurance Certification and Accreditation Process
DoD.....	Department of Defense
DoDD.....	Department of Defense Directive
DoDI	Department of Defense Instruction
IA	Information Assurance
IAVM.....	Information Assurance Vulnerability Management
IAWG.....	Information Assurance Working Group
IM.....	Information Management
IS.....	Information System
IT.....	Information Technology
JMISO.....	Joint Medical Information Systems Office
MAC	Mission Assurance Category
MHS.....	Military Health System
OCIO.....	Office of the Chief Information Officer
PEO.....	Program Executive Office
PHI	Protected Health Information
PK	Public Key
PKI	Public Key Infrastructure
TMA.....	TRICARE Management Activity
TRO.....	TRICARE Regional Offices
VHA.....	Veterans Health Administration