



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](mailto: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;"><b>MILITARY HEALTH SYSTEM (MHS) INFORMATION ASSURANCE (IA) IMPLEMENTATION GUIDE</b></p>	<b>IMPLEMENTATION GUIDE No. 10</b>	
	<b>EFFECTIVE DATE 07/19/05</b>	<b>REVISED DATE 10/10/08</b>
<p><b>Subject:</b></p> <p style="text-align: center;"><b>SYSTEM LIFE CYCLE MANAGEMENT</b></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 policies and procedures.

1.2. The MHS Information Assurance (IA) System Life Cycle Management (LCM) process ensures required security safeguards are developed and executed to protect Information Systems (ISs) against accidental or intentional unauthorized modification, disclosure, destruction, and denial of service throughout the life cycle of the system. Including security early in the IS development life cycle, rather than adding it to an operational system, will usually result in less expensive and more effective security.

1.3. This implementation guide provides direction on the scope of IA elements to be considered during the system development life cycle and when integrating IA into the acquisition process. IA shall be considered in all phases of the LCM process and shall be included in the preliminary acquisition implementation strategy. Identifying IA safeguards early in the acquisition implementation strategy will ensure that key elements, such as technical security requirements, scheduling, and cost and funding issues associated with executing requirements for IA are addressed and maintained. IA requirements shall be incorporated in the early stages of program design activities to ensure the appropriate confidentiality, integrity, availability, authenticity, and non-repudiation of the system information are protected in accordance with Department of Defense (DoD) policy. As part of the incorporation of IA in the early stages, the Certification and Accreditation (C&A) staff should be included in the process to ensure C&A can be completed smoothly. IA is considered an integral segment of security LCM and the acquisition process.

## **2. POLICY**

2.1. It is MHS Policy that:

2.1.1. IA requirements be identified and included in the design, acquisition, installation, operation, and upgrade or replacement of MHS ISs.

2.1.2. Required IA Controls be implemented to protect MHS ISs against unauthorized modification, disclosure, destruction, and denial of service throughout the security development life cycle phases.

2.1.3. As early as possible in the life cycle of IT-dependent programs, information owners shall establish the Mission Assurance Category (MAC), security classification, sensitivity, and need-to-know of information and information systems.

2.1.4. The IA controls be established as part of the baseline requirements consistent with DoDI 8500.2, "Information Assurance (IA) Implementation," February 6, 2003, and are implemented throughout the system's life cycle. DoDI 8500.2 provides a detailed list of the IA controls necessary to achieve the baseline levels of confidentiality, integrity, and availability.

2.1.5. TMA Components shall, at a minimum:

2.1.5.1. Develop security specifications based on DoD IA Controls.

2.1.5.2. Identify risk areas and define risk reduction measures, management approaches, and plans.

2.1.5.3. Test and evaluate to certify that technical security features and other safeguards satisfy specified security requirements before the initiation of operational testing.

2.1.5.4. Establish procedures to ensure continuous use of approved security safeguards during the production, deployment, implementation, and operational/maintenance phases.

2.1.5.5. Ensure IA requirements are addressed and incorporated into the acquisition documentation in accordance with: DoDD 5000.01, "The Defense Acquisition System," May 12, 2003, DoDD 5000.02, "Operation of the Defense Acquisition System," May 12, 2003, and DoDI 8580.1, "Information Assurance (IA) in the Defense Acquisition System," July 9, 2004.

## **3. PROCEDURES**

3.1. IA LCM incorporates operational requirements for security in all IS planning and design, and ensures conformance with applicable security regulations, policies, and requirements. The product of this activity is the Information Assurance Strategy. The TMA Component sponsoring the system development shall have an understanding of the nature, need, and information processed by the system to determine the information's sensitivity and criticality.

3.1.1. Security System Life Cycle Management Phases - Security planning shall be implemented throughout a system life cycle. This begins with the DoD Information Assurance Certification and Accreditation Process (DIACAP) as referenced in DoDI 8510.01, "DoD Information Assurance Certification and Accreditation Process (DIACAP)," November 28, 2007. The DIACAP parallels the system life cycle, and its activities should be initiated at inception (e.g., documented during capabilities identification or at the implementation of a major system modification).

3.1.2. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. At a minimum, the TMA Component shall incorporate the following security into the system life cycle:

3.1.2.1. Initiate and Plan the Certification and Accreditation (C&A)

3.1.2.1.1. This activity includes registering the system with the governing DoD and DoD Component IA programs, assigning IA controls based on Mission Assurance Category (MAC) and Confidentiality Level (CL), identifying the DIACAP Team for the IS, and initiating the IS's DIACAP Implementation Plan.

3.1.2.1.2. System registration establishes the relationship between the DoD IS and the governing DoD Component IA program which continues until the DoD IS is decommissioned. The System Identification Profile (SIP) is generated during the registration process and becomes part of the DIACAP package for the IS.

3.1.2.2. Implement and Validate Assigned IA Controls

3.1.2.2.1. IA Controls Analysis – analysis of IA controls that address the required development activities and the assurance evidence needed to produce the desired level of confidence in the accuracy and effectiveness of the information security. This analysis shall ultimately become part of the baseline IA security requirements.

3.1.2.2.2. IA Control Development – ensures that IA controls are described in the security plans and are implemented consistent with the DoD. For ISs currently in operation (e.g., legacy systems), the security plans may call for additional IA controls or modification of existing IA controls.

3.1.2.2.3. This activity includes executing the DIACAP Implementation Plan (DIP), conducting validation activities, preparing the IT Security Plan of Action & Milestones (POA&M), and compiling the validation results in the DIACAP Scorecard.

3.1.2.3. Make Certification Determination and Accreditation Decision

3.1.2.3.1. The certification determination is based on the actual validation results. It considers impact codes associated with IA controls in a non-compliant status, associated severity categories, expected exposure time (i.e., the projected life of the system

release or configuration minus the time to correct or mitigate the IA security weakness), and cost to correct or mitigate (e.g., dollars, functionality reductions). The weaknesses identified on the IT Security POA&M reflect residual risk to the system.

3.1.2.3.2. A certification determination is always required before an accreditation decision. If a compelling mission or business need requires the rapid introduction of a new DoD IS into the Global Information Grid (GIG), validation activity and a certification determination are still required.

3.1.2.3.3. Inspection and Acceptance – ensures that the MHS Office of the Chief Information Officer/Information Assurance (OCIO/IA) and local Designated Accrediting Authority (DAA) validate and verify that the functionality described in the specification is included in the deliverables.

3.1.2.3.4. The DAA issues accreditation decisions.

#### 3.1.2.4. Maintain Authorization to Operate and Conduct Reviews

3.1.2.4.1. Continued Authorization To Operate is contingent on the sustainment of an acceptable IA posture. The DoD IS Information Assurance Manager (IAM) has primary responsibility for maintaining situational awareness and initiating actions to improve or restore IA posture.

3.1.2.4.2. Maintain Situational Awareness. Included in the IA controls assigned to all DoD ISs are IA controls related to configuration and vulnerability management, performance monitoring, and periodic independent evaluations (e.g., penetration testing).

3.1.2.4.3. The IAM may recommend changes or improvement to the implementation of assigned IA controls, the assignment of additional IA controls, or changes or improvements to the design of the IS itself.

3.1.2.4.4. The IAM shall annually provide a written or DoD Public Key Infrastructure (PKI)-certified digitally signed statement to the DAA and the Certifying Authority (CA) that indicates the results of the security review of all IA controls and the testing of selected IA controls.

#### 3.1.2.5. Decommission

3.1.2.5.1. When a DoD IS is removed from operation, a number of DIACAP related actions are required. Prior to decommissioning, any inheritance relationships should be reviewed and assessed for impact.

3.1.2.5.2. Once the system has been decommissioned, the SIP should be updated to reflect the IS decommissioned status.

3.1.2.5.3. Concurrently, the DIACAP Scorecard and any POA&M should also be removed from all tracking systems. Other artifacts and supporting documentation should be disposed of according to its sensitivity or classification. Data or objects in IA infrastructures that support the GIG, such as key management, identity management, vulnerability management, and privilege management, should be reviewed for impact.

### 3.1.2.6. Information Disposition

3.1.2.6.1. Information Preservation – ensures that information is retained, as necessary, to conform to the DoD sensitive information protection requirements.

3.1.2.6.2. Media Sanitization – ensures that hardware and software are disposed of in accordance with current DoD policy and the applicable MHS IA policy implementation guide. To mitigate the potential risk and vulnerabilities, the following procedures must be followed prior to releasing custody or transferring the electronic storage media and IT equipment. This procedure also applies to contractor-supplied IT equipment and electronic storage media.

3.1.2.6.3. Computer Transfer or Disposition - Before a computer system is sold, transferred, or otherwise disposed of, all sensitive and/or confidential program or data files on any storage media must be completely erased or otherwise made unreadable in accordance with: ASD(C3I) Memorandum, “Disposition of Unclassified DoD Computer Hard Drives,” June 4, 2001 and DoD 5220.22-M, “National Industry Security Program Operating Manual (NISPO),” February 28, 2006.

3.1.2.6.4. The computer system must be relocated to a designated, continuous physically secure storage area in accordance with DoD 5200.1-R, “Information Security Program”, January 14, 1997 until sanitization is completed.

3.1.2.6.5. The term of the license agreement must be complied with whenever software licenses are negotiated with the transfer of equipment or media, or the disposition thereof.

3.1.2.6.6. Once the sanitization is complete, the process must be certified and the record maintained for a period of six years.

### 3.1.2.7. MHS IA Program Considerations

3.1.2.7.1. Security Functional Requirements Analysis – analysis of requirements that may include the following components: (1) system security environment (policies and architecture) and (2) security functional requirements.

3.1.2.7.2. Cost Consideration and Reporting – determines the amount of development attributed to information security over the life cycle of the system. This cost includes hardware, software, personnel, and training.

3.1.2.7.3. Other Planning Components – ensures that all components of the development process are considered when incorporating IA into the life cycle. These selections include appropriate contract type, participation by all related functional groups, participation by CA and DAA and development and execution of necessary contracting plans and process.

## 3.2. Acquisition Program Manager (PM) Responsibilities

3.2.1. At a minimum, the PMs for acquisition programs shall:

3.2.1.1. Remain ultimately responsible for the platform’s overall IA protection for acquisitions of platform IT systems (e.g., medical technologies or utility distribution systems) with internal IT components.

3.2.1.2. Retain responsibility to incorporate all IA protective measures necessary to support the platform’s support mission functions for acquisitions of platforms with IT that do not interconnect with external networks.

3.2.1.3. Identify all assurance measures needed to ensure both the protection of the network and the protection of the platform from connection risks, such as unauthorized access, that may be introduced from the network.

3.2.1.4. Demonstrate prudent judgment by considering the IA program provisions in DoD Directive (DoDD) 8500.01E, and DoDI 8500.2, for systems that are not connected to external networks and that do not involve internal networks, and employing those IA controls appropriate to their system.

3.2.1.5. Be responsible for coordinating with enclaves that host Automated Information Systems (AISs) applications early in the acquisition process to address operational security risks the system may impose upon the enclave, as well as identifying all system security needs that may be more easily addressed by enclave services than by system enhancement.

3.2.1.6. Comply with the IA requirements in the DoD 8500 policy series for acquisitions of outsourced IT-based processes.

3.2.1.7. Be responsible for employing the sets of baseline controls appropriate to their programs.

## 4. **REFERENCES**

1. ASD (C3I) Memorandum, “Disposition of Unclassified DoD Computer Hard Drives,” June 4, 2001
2. DoDD 5000.01, “The Defense Acquisition System,” May 12, 2003
3. DoDI 5000.02, “Operation of the Defense Acquisition System,” May 12, 2003

4. DoDI 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” November 28, 2007
5. DoDD 8500.01E, “Information Assurance (IA),” October 24 2002, Certified Current as of April 23, 2007
6. DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
7. DoDI 8580.1, “Information Assurance (IA) in the Defense Acquisition System,” July 9, 2004
8. DoD 5200.1-R, “Information Security Program,” January 14, 1997
9. DoD 5220.22-M, “National Industry Security Program Operating Manual (NISPOM),” February 28, 2006

## 5. ACRONYMS

AIS .....	Automated Information System
ASD.....	Assistant Secretary of Defense
C&A.....	Certification and Accreditation
CA.....	Certifying Authority
CL .....	Confidentiality Level
DAA.....	Designated Accrediting Authority
DIACAP.....	DoD Information Assurance Certification and Accreditation Process
DIP .....	DIACAP Implementation Plan
DoD.....	Department of Defense
DoDD.....	Department of Defense Directive
DoDI .....	Department of Defense Instruction
GIG .....	Global Information Grid
IA .....	Information Assurance
IAM.....	Information Assurance Manager
IS .....	Information System
IT.....	Information Technology
JMIS.....	Joint Medical Information Systems
LCM.....	Life Cycle Management
MAC .....	Mission Assurance Category
MHS.....	Military Health System
NISPOM .....	National Industry Security Program Operating Manual
OCIO.....	Office of the Chief Information Officer
PEO.....	Program Executive Office
PKI .....	Public Key Infrastructure
PM.....	Program Manager
POA&M.....	Plan of Action & Milestones
SIP.....	System Identification Profile
TMA.....	TRICARE Management Activity