



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

FEB 23 2010

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 19 July 2005, this office has completed a review of the MHS IA Policy Guidance and Implementation Guides. As a result, the following documents have been updated:

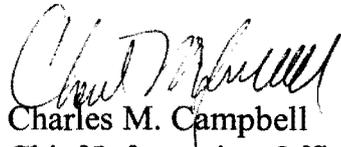
Information Assurance (IA) Policy Guidance
Implementation Guide No. 3, "Incident Reporting"
Implementation Guide No. 8, "Certification and Accreditation"

The MHS IA Policy Guidance and IA Implementation Guides were developed in collaboration with the MHS IA Working Group.

The provisions of the MHS IA Policy Guidance and IA Implementation Guides are policy for all TRICARE Management Activity (TMA) Directorates, TRICARE Regional Offices (TRO), 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, Director,
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. 8	
	EFFECTIVE DATE 07/19/05	REVISED DATE 02/02/10
<p>Subject:</p> <p style="text-align: center;">CERTIFICATION AND ACCREDITATION (C&A)</p>		

1. PURPOSE AND SCOPE

1.1 The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (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 (CIO) of the Service Medical Departments are encouraged to incorporate this document into their information assurance polices and procedures.

1.2 The MHS C&A process is conducted in accordance with DoDD 8500.01E, “Information Assurance (IA),” (reference (b)) and DoDI 8510.01, “DoD Information Assurance Certification and Accreditation Process (DIACAP),” (reference (a)). DIACAP parallels the system lifecycle and encompasses five primary activities; Initiate and Plan Information Assurance (IA) C&A, Implement and Validate Assigned IA Controls, Make Certification Determination and Accreditation Decision, Maintain Authorization To Operate and Conduct Reviews, and Decommission. DIACAP applies to all the TMA Component and contractor information systems (ISs), including networks (henceforth referred to as ISs). The primary purpose of DIACAP is to protect and secure the elements that make up the MHS information infrastructure, regardless of where the IS is located. DIACAP procedures shall be utilized in conjunction with DoDI 8500.2, “Information Assurance (IA) Implementation,” (reference (c)). All DoD ISs shall be reaccredited within three years of the effective Authorization to Operate (ATO) or when significant changes occur to impact the security posture of the systems. The MHS C&A process must be monitored and maintained throughout the system’s development life cycle. Key information technology (IT) personnel shall adhere to the MHS C&A process for any government-owned or contractor-owned IS that transmits, processes, stores, or accesses DoD information and/or connects to any DoD system or network during acquisition, operation, and throughout the system life cycle.

2. **POLICY**

2.1 The MHS shall conduct C&A for all MHS ISs (government-owned or contractor-owned) that transmit, process, store, or access DoD information and/or connect to any DoD system or network. The MHS IA Program also requires TRICARE contractors to comply with C&A requirements. The MHS shall utilize current DoD C&A guidance as its baseline to maintain a sound IA posture throughout the MHS IS infrastructure. Throughout all the phases of MHS ISs development, information owners must include and utilize the guiding principles of current DoD C&A guidance.

2.2 The MHS IA Program Office shall ensure that all planning activities are scheduled and maintained to ensure MHS ISs that require C&A are managed effectively. The registration and management of ports, protocols, and services shall also be addressed as part of the C&A process. Upon recommendation from their respective Certifying Authorities (CAs), the Designated Accrediting Authorities (DAAs) shall authorize, via letter to the MHS IS Program Managers (PM), an Authorization To Operate (ATO) for a maximum period of three years, an Interim Authorization To Operate (IATO) for 180 days, an Interim Authority to Test (IATT) or a Denial of Authorization To Operate (DATO). The Designated Accrediting Authority (DAA) may not grant consecutive IATOs totaling more than 360 days.

2.3 A Certifying Authority shall be designated by the DAA with the authority to establish and manage the organization's C&A program and to verify and validate IS security design and implementation through testing and review of IS security documentation. An annual review will be performed as a part of the C&A process to review artifacts, changes to DoD Ports, Protocols, and Services Management, and security controls. Approximately seven months prior to the expiration of the system's accreditation, or when significant changes occur or are projected to occur, the PM, System Owner, and contractor Point of Contact (POC) must request reaccreditation or an IATO from the MHS IA Program Office. An IATO is reserved for ISs that have not been certified or accredited, and yet for operational reasons, must be deployed before completing certification or accreditation, or for accredited systems that cannot complete their recertification before their current certification expires.

2.4 The Office of the Chief Information Officer (OCIO)/IA Document Management Exchange (DMXchange) is the official repository for TMA and TRICARE Contractor DIACAP documents and artifacts and the MHS IA Trends Analysis Database (TAD) is the official repository for IA assessment data. TMA Program Managers and TRICARE Contractors shall ensure that requisite documentation is entered and maintained in these systems.

3. **RESPONSIBILITIES**

3.1 The Director, MHS shall:

3.1.1 Ensure all MHS ISs comply with the DIACAP.

3.1.2 Operate only accredited ISs.

3.1.3 Comply with all accrediting decisions, including denial of authorization to operate (DATO), and enforce authorization termination dates (ATDs).

3.2 The MHS Chief Information Officer (CIO) shall:

3.2.1 Appoint a Senior Information Assurance Officer to direct and coordinate the MHS IA program consistent with the strategy and direction of the Defense-wide Information Assurance Program (DIAP).

3.2.2 Ensure that the C&A status of MHS ISs is visible to the Assistant Secretary of Defense for Network and Information Integration (ASD(NII))/DoD CIO and Principal Accrediting Authorities (PAA).

3.2.3 Ensure a DIACAP scorecard with a manual or DoD Public Key Infrastructure (PKI) certified digital signature is visible to the DoD CIO. The DIACAP Scorecard shall document the DAA accreditation decision as well as the results of the implementation of required baseline IA controls and any additional IA controls that may be required locally.

3.2.4 Ensure an Information Technology (IT) Security Plan of Action and Milestones (POA&M) is developed and maintained to record the status of any corrective actions directed in association with an accreditation decision.

3.2.5 Ensure all MHS ISs with an Authorization To Operate (ATO) are reviewed annually to confirm that the IA posture of the IS remains acceptable. Reviews will include validation of IA controls and be documented in writing.

3.2.6 Ensure contracts for systems, services, and programs covered by DoDI 8510.01, (reference (a)), include clauses requiring compliance with the DIACAP.

3.3 The Director MHS IA Program shall:

3.3.1 Ensure TMA and TRICARE contractor ISs are accredited and undergo reaccreditation every three years, or sooner in the event that significant changes occur to impact the security posture of the system.

3.3.2 Contact the PM, System Owner, and contractor POC, prior to when the IS is scheduled for an annual review or recertification.

3.3.3 Provide assistance and guidance, when necessary, to programs and projects that are preparing for, undergoing, and complying with current DoD C&A requirements.

3.4 Service Medical Chief Information Officers shall:

3.4.1 Ensure their respective Service-specific ISs and contractor ISs are certified and accredited and undergo reaccreditation every three years, or sooner in the event that significant changes occur to impact the security posture of the system.

3.4.2 Contact the PM and/or contractor POC prior to when the IS is scheduled for an annual review or recertification.

3.4.3 Provide assistance and guidance, when necessary, to programs and projects that are preparing for, undergoing, and complying with current DoD C&A requirements.

3.5 The JMISO PEO shall:

3.5.1 Ensure TMA Centrally Managed ISs are certified and accredited and undergo re-accreditation every three years, or sooner in the event that significant changes occur to impact the security posture of the system.

3.5.2 Contact the PM, System Owner, and contractor POC prior to when the IS is scheduled for an annual review or recertification.

3.5.3 Provide timely coordination, assistance, and guidance, when necessary, to programs and projects that are preparing for, undergoing, and complying with current DoD C&A requirements.

3.6 The Senior Information Assurance Officer (SIAO) shall:

3.6.1 Establish and enforce the C&A process within the MHS IA program.

3.6.2 Ensure MHS-level participation in the DIACAP Technical Advisory Group (TAG).

3.6.3 Track the C&A status of ISs that are governed by the MHS IA program.

3.6.4 Establish and manage a coordinated IA certification process for ISs governed by the MHS IA program.

3.6.5 Serve as the single IA coordination point for joint or Defense-wide programs that are deploying ISs to MHS enclaves.

3.7 The DAA shall:

3.7.1 Ensure a DIACAP package is initiated and completed for all MHS ISs.

3.7.2 Ensure ISs comply with applicable DoD baseline IA controls.

3.7.3 Authorize or deny operation or testing of MHS ISs. Coordinate with the Director, Operational Test and Evaluation before denying an IATT.

3.7.4 Ensure that Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) are appointed in writing and are designated for all systems under their jurisdiction, and that they receive the level of training and certification necessary to perform the tasks associated with their assigned responsibilities.

3.7.5 Ensure the reaccreditation of ISs and networks at least every three years, or whenever previously accredited systems undergo major modifications.

3.7.6 Verify that an appropriate mission assurance category has been assigned for each IS/network under his/her jurisdiction.

3.8 Program Managers shall:

3.8.1 Implement the DIACAP for assigned ISs.

3.8.2 Enforce DAA accreditation decisions for hosted or interconnected ISs.

3.8.3 Develop, track, resolve, and maintain the DIACAP Implementation Plan for assigned ISs.

3.8.4 Ensure IT Security POA&M development, tracking, and resolution.

3.8.5 Ensure annual reviews of assigned ISs required by the DoDI 8510.01, (reference (a)), are conducted. The annual review shall include testing the contingency plan. Contingency planning refers to interim measures to recover IT services following an emergency or system disruption. NIST Special Publication 800-34, "Contingency Planning Guide for Information Technology (IT) Systems," (reference (d)), provides instructions, recommendations, and considerations for government IT contingency planning. Contingency planning IA controls and validation procedures may be found in DoDI 8500.2, (reference (c)).

3.8.6 Provide resources to perform C&A of systems, applications, and networks under their control throughout the life cycle.

3.8.7 Utilize guidance specified in this document and detailed instructions in references in Section 6.

3.8.8 Ensure C&A is accomplished prior to deployment of newly developed ISs and/or networks.

3.8.9 Ensure a risk assessment is performed as part of the C&A.

3.8.10 Maintain ISs' security controls to comply with current DoD IA policies and directives.

3.8.11 Identify security deficiencies and take action to achieve an acceptable security level.

3.8.12 Verify data ownership, accountability, and access rights, and ensure all special handling requirements are established for each IS/network under his/her jurisdiction.

3.8.13 Ensure that all Health Insurance Portability and Accountability Act (HIPAA) Security requirements are met for all ISs/networks that process, store, transmit, or access protected health information (PHI).

3.8.14 Ensure processes for reporting security incidents and lessons learned are established in accordance with the MHS Incident Reporting and Response Program Implementation Guide, No. 3, (reference (e)).

3.8.15 Ensure that security safeguards approved during accreditation are implemented and maintained as necessary throughout the system life cycle.

3.8.16 Ensure that an IA awareness, training, and education program is implemented for all users, to include developers, SAs, operators, and managers.

3.8.17 Document Memorandums of Agreement (MOAs) and Memorandums of Understanding (MOUs) to address security requirements between ISs that interface or are networked and managed by different DAAs.

3.8.18 Document MOAs and MOUs to address security requirements between ISs that are interfaced or networked to non-DoD entities. If these connections process PHI, then appropriate Business Associate Agreements addressing HIPAA Security requirements must also be in place.

3.9 The Certifying Authority shall:

3.9.1 Establish and manage the C&A program.

3.9.2 Ensure verification and validation of IS security design and implementation through testing and review of the IS security documentation.

3.9.3 Ensure compliance with the following Defense Information Systems Agency (DISA) products. DISA Security Technical Implementation Guides (STIGs) are the configuration standards for DoD IA and IA-enabled devices/systems. Security Checklists (sometimes referred to as lockdown guides, hardening guides, or benchmark configuration) are documents that contain instructions or procedures to verify compliance to a baseline level of security. STIGs and checklists may be found at the DISA Information Assurance Support Environment (IASE) web site <http://iase.disa.mil.stigs/index.html>.

3.9.4 Review C&A artifacts and security controls on an annual basis, or when significant changes occur.

3.9.5 Prepare the DIACAP Executive Package with system certification recommendations for the DAA.

4. IA SECURITY REQUIREMENTS

4.1 IA Security requirements shall be established for all MHS ISs. Security requirements shall consist of, but are not limited to, administrative, personnel, physical, environmental, and technical controls which shield the IS against sabotage, tampering, denial of service, espionage, fraud, misappropriation, misuse, modification, destruction, and data disclosure. The security requirements shall be satisfied through a combination of administrative, automated, and manual means in a cost-effective and integrated fashion. All TMA Component and contractor ISs shall be evaluated to ensure minimum security standards are implemented and enforced in accordance with references in Section 6.

5. REACCREDITATION

5.1 In accordance with current DoD C&A procedures, ISs shall be reaccredited every three years, or sooner if a significant change to hardware, software, or environment occurs. The following is a list of events affecting security that may require ISs to be recertified and reaccredited:

5.1.1 Level of criticality and/or sensitivity change for the system/environment impacting reliable baseline countermeasures.

5.1.2 Hardware additions, changes, or upgrades requiring a change in the approved security countermeasures.

5.1.3 Software (operating system or applications) additions, changes, or upgrades (e.g., additional functional and capability modules).

5.1.4 Security policy (e.g., access control policy) changes.

5.1.5 Threat change creating system vulnerability resulting in a higher risk.

5.1.6 Mission changes requiring a different security mode of operation.

5.1.7 Breaches of security, system integrity, or unusual situations that appear to invalidate the accreditation by revealing flaws in security design exposing its vulnerability.

5.1.8 Significant changes in the physical structure of the facility or the system is moved to a different facility.

5.1.9 Significant changes in operating procedures.

5.1.10 System configuration changes (e.g., a workstation connected outside of the approved accreditation parameters).

5.1.11 Networks - Inclusion of additional (separately accredited) system(s) affecting the security of that system.

5.1.12 Networks - Modification/replacement of a subscribing system affecting the security of that system.

5.1.13 Results of an audit or external analysis.

5.1.14 Addition of system interfaces with other systems.

6. **REFERENCES**

- a. DoD Instruction 8510.01, DoD Information Assurance Certification and Accreditation Process (DIACAP),” 28 November 2007
- b. DoD Directive 8500.01E, “Information Assurance (IA),” 24 October 2002, Certified Current as of 23 April 2007
- c. DoD Instruction 8500.2, “Information Assurance (IA) Implementation,” 6 February 2003
- d. NIST Special Publication 800-34, “Contingency Planning Guide for Information Technology (IT) Systems,” June 2002
- e. MHS Implementation Guide No. 3, “Incident Reporting and Response Program,” 7 January 2010
- f. STIGs and Checklist, DISA Information Assurance Support Environment (IASE) web suit, <http://iase.disa.mil.stigs/index.html>, current

7. **ACRONYMS**

ASD(NII)	Assistant Secretary of Defense for Network and Information Integration
ATO	Authorization to operate
ATD	Authorization Termination Date
C&A	Certification and Accreditation
CA	Certifying Authority
CIO	Chief Information Officer
DAA	Designated Accrediting Authority
DATO	Denial of Authorization To Operate
DIACAP	DoD Information Assurance Certification and Accreditation Process
DIAP	Defense-wide Information Assurance Program
DISA	Defense Information Systems agency
DMXchange	Document Management Exchange
DoD	Department of Defense

DoDDDepartment of Defense Directive
 DoDIDepartment of Defense Instruction

 FISMAFederal Information Security Management Act

 HIPAAHealth Insurance Portability and Accountability Act

 IAInformation Assurance
 IAM.....Information Assurance Manager
 IAOInformation Assurance Officer
 IASE.....Information Assurance Support Environment
 IATO.....Interim Authorization To Operate
 IATT.....Interim Authorization To Test
 ISInformation System
 IT.....Information Technology

 JMISO.....Joint Medical Information Systems Office

 MHSMilitary Health System
 MOAMemorandum of Agreement
 MOUMemorandum of Understanding

 PAA.....Principal Accrediting Authorities
 PEO.....Program Executive Officer
 PHIProtected Health Information
 PKIPublic Key Infrastructure
 PM.....Program Manager
 POA&M.....Plan Of Action and Milestones
 POC.....Point of Contact

 SASystem Administrator
 SIAO.....Senior Information Assurance Officer
 SRR.....Security Readiness Review Scripts
 STIG.....Security Technical Implementation Guides

 TADTrends Analysis Database
 TAGTechnical Advisory Group
 TMA.....TRICARE Management Activity
 TRO.....TRICARE Regional Offices