



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
WASHINGTON, DC 20301-1200

MAR 27 2007

MEMORANDUM FOR TRICARE MANAGEMENT ACTIVITY
PROGRAM EXECUTIVE OFFICE 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 the bi-annual review of the MHS IA Policy Guidance and Implementation Guides. As a result, the following documents have been updated:

Military Health System (MHS) Information Assurance (IA) Policy Guidance
Implementation Guide No. 3, "Incident Reporting and Response Program"
Implementation Guide No. 4, "Employee Behavior"
Implementation Guide No. 7, "Data Integrity"
Implementation Guide No. 8, "Certification and Accreditation (C&A)"
Implementation Guide No. 12, "Information Assurance Vulnerability
Management (IAVM) Program"
Implementation Guide No. 13, "Information Assurance Training, Education, and
Awareness"
Implementation Guide No. 14, "Information Operation Condition (INFOCON)
Standard Operating Procedures"

The MHS IA Policy Guidance and 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 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. They will be reviewed bi-annually and updated as needed.

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 polices 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.



Carl E. Hendricks
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

Military Health System Information Assurance Policy Guidance



27 March 2007

**Prepared By:
Military Health System
Information Assurance Program Office**

Military Health System (MHS) Information Assurance (IA) Policy Guidance

SUBJECT: Information Assurance (IA)

References:

- a. DoDD 8500.1, "Information Assurance (IA)," 24 October 2002
- b. DoDI 8500.2, "Information Assurance (IA) Implementation," 6 February 2003
- c. Interim Department of Defense Information Assurance Certification and Accreditation Process (DIACAP) Guidance, 6 July 2006
- d. "Military Health System Information Assurance Policy Guidance," 5 March 2004 (hereby canceled)
- e. through (y.), see Enclosure 1

1 PURPOSE

- 1.1 This document establishes guidance and assigns the roles and responsibilities needed to ensure that sufficient security safeguards are implemented within the Military Health System (MHS) to comply with DoDD 8500.1, "Information Assurance (IA)" (reference a.) and the Department of Defense (DoD) Defense-in-Depth IA strategy. Adherence to the provisions in this guidance ensures that an appropriate and consistent level of security is achieved to maintain availability, integrity, authentication, confidentiality, and non-repudiation of the MHS' Information Systems (ISs). As per DoDD 8500.1, "Information Assurance (IA)," and Enclosure 2 (Definitions), the term "Information System" encompasses all Automated Information System Applications, Enclaves, Outsourced Information Technology (IT)-based Processes, and Platform IT Interconnections. The information systems within the MHS will be assigned a Mission Assurance Category as well as a Confidentiality Level and must comply with the IA controls established in DoDI 8500.2, "Information Assurance (IA) Implementation," (reference b.). Medical information has been designated as Sensitive Information (SI), and is to be handled in accordance with this guidance.
- 1.2 This guidance directly supports the mission of the MHS and the TRICARE Management Activity (TMA) by applying the principles of DoD information and technology management. This includes developing and implementing policies, procedures, programs, and technical standards necessary to acquire, manage, integrate, and secure information technology systems and capabilities that support the delivery of high quality, cost effective health care services across the operational continuum. It incorporates security safeguards directed by the federal government and the DoD, and provides information on security best practices developed as a result of several partnerships. Some of those partners include the DoD, National Institute of Standards and Technology (NIST), National Security Agency, corporate America, and other organizations committed to sharing best practices in efforts to achieve IA on a global scale.

- 1.3 This guidance supersedes the “Military Health System Information Assurance Policy Guidance, 5 March 2004” (reference d.), in its entirety.

2 SCOPE

- 2.1 The provisions of this document are policy for all TMA Directorates; TRICARE Regional Offices (TRO); and the Joint Medical Information Systems (JMIS) Office (hereafter collectively 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. This document applies to the organization, its military personnel, DoD civilians, and contractors, who manage, design, develop, operate, or access DoD ISs, and TMA developed and operated ISs, or access DoD data. Additionally, ISs include:
 - 2.1.1 MHS information systems that support special environments, such as the Defense Blood Standard System (DBSS), which supports the blood bank at Military Treatment Facilities (MTFs).
 - 2.1.2 Platform IT interconnections, e.g., sensors, medical technologies, or utility distribution systems, to external networks. Platform IT interconnections have readily identifiable security implications, essential to mission performance, and provide data exchange to enclaves. An example of a Platform IT interconnection might be a lab device that stores protected health information (PHI) and interconnects to the network.
 - 2.1.3 Information systems under contract to the MHS.
 - 2.1.4 Outsourced information-based processes such as those supporting e-Business or e-Commerce processes.
 - 2.1.5 Stand-alone information systems.
 - 2.1.6 Mobile computing devices such as laptops, handhelds, and personal digital assistants operating in either wired or wireless mode, and other information technologies as may be developed.
 - 2.1.7 Biomedical technologies/devices that may or may not interconnect with a network, but process and store sensitive information.

3 GUIDANCE

- 3.1 The MHS protects the availability, integrity, authentication, confidentiality, and non-repudiation of information processed on ISs and effectively and efficiently manages the risks encountered by the MHS.

- 3.2 TMA Components shall conduct a thorough investigation and inventory of their respective organizations to determine where DoD data is accessed, stored, received, processed, or transmitted in order to provide the requisite protection as required by this guidance. Areas of concern include but are not limited to: sites where transcription coding services take place (individual homes), bio-medical and wireless devices, networks, workstations, and special servers outside of the network.
- 3.3 Security Life Cycle Management
- 3.3.1 The MHS Information Assurance (IA) System Life Cycle Management (LCM) process ensures required security safeguards are developed and executed to protect 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.
- 3.3.2 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.
- 3.4 Governance - The MHS IA Program governance consists of those functions that contribute to the effective implementation of the IA program. They are program management, planning, budgeting, staffing, and performance measurement.
- 3.4.1 Program Management – The MHS IA Program Office shall create, program, budget, operate, maintain, and measure the performance of an IA Program that provides strategic and tactical IA direction, plans, and objectives.
- 3.4.2 Program Planning – During the creation of the Program Objective Memorandum (POM), IA requirements shall be included for each support system, application, and IT system to ensure adequate resources are available for IT programs during their entire life cycle.
- 3.4.3 Program Budgeting – All TMA Components shall budget and account for IA requirements and expenditures in the support of managing risk to their IT assets.
- 3.4.4 Program Staffing – Staffing of the MHS IA Program shall be limited to highly qualified and certified IA professionals. The skill mix of the team must ensure competency in planning, programming, budgeting, budget execution, and performance measurement. The IA staff may function as project and contract managers for IA support and services developed or acquired by the MHS.

- 3.4.5 Program Performance Measurement – Processes shall be established, implemented, and managed by the MHS IA Program Office that will provide executive leadership with a view of how well the IA program is working throughout the MHS.
- 3.5 Certification and Accreditation (C&A)
- 3.5.1 All ISs governed by this guidance are subject to a comprehensive Certification and Accreditation process in accordance with “Interim Department of Defense Certification and Accreditation Process (DIACAP) Guidance” (reference c.).
- 3.5.2 All DOD ISs shall be reaccredited at least every three years, or more frequently if deemed necessary due to IS modifications or changes in the operating environment.
- 3.6 Risk Management – Assessing risk ensures that new threats and vulnerabilities are identified and appropriate security countermeasures are implemented. Risk assessments shall be conducted whenever significant and major changes occur or when new threats are identified to the DoD IS or the IS operating environment.
- 3.6.1 Risk Analysis – When a change is made that may impact security posture, TMA Components shall conduct an independent full risk analysis and assessment of each of their ISs to identify potential new vulnerabilities and to verify current security safeguards continue to provide adequate protection.
- 3.6.2 Penetration Testing – TMA Components shall attempt to exploit network security vulnerabilities using penetration testing during the C&A process, or more frequently as required by the MHS IA Program Office. Penetration tests on DoD ISs will be conducted by the MHS IA Program Office, in coordination with the appropriate Service, to verify the adequacy of security counter measures in place.
- 3.6.3 Vulnerability Assessments – TMA Components shall identify system and network vulnerabilities through use of vulnerability assessment tools. Vulnerability assessments shall be conducted on the network and critical servers and systems at least annually.
- 3.6.4 Contingency Plans – TMA Components shall incorporate contingency plans as a part of their IS security program to ensure the availability of critical resources and facilitate the continuity of operations during an emergency or during an unexpected event. For additional Contingency Planning guidance, refer to NIST Special Publication 800-34, “Contingency Planning Guide for Information Technology Systems” (reference u).
- a. Information Assurance Officers (IAOs) and System Administrators (SAs) shall coordinate the development of contingency plans that address Continuity of Operations Plans and Disaster Recovery Plans.
 - b. Management at all echelons, including Information Assurance Managers (IAMs), IAOs and SAs must actively participate in the planning and testing of contingency plans at least annually.

- c. Plans must be tested under realistic operational conditions; the results of such tests shall be documented.

3.6.5 Configuration Management – TMA Components shall develop, implement, and maintain a configuration management plan that is defined in the System Security Authorization Agreement (SSAA). Detailed guidance exists in National Computer Security Center – Technical Guidance (TG)-006, “A Guide to Understanding Configuration Management in Trusted Systems” (reference s.) and in Military Handbook (MIL-HDBK) - 61A, “Configuration Management Guidance” (reference r.).

- a. No changes to the configuration of an IS shall be made until the IAO evaluates the effect(s) the proposed change will have on the security countermeasures in place on the IS, and the Designated Accrediting Authority (DAA) grants approval for the change. The approval must be formally documented and reflected in the SSAA.
- b. During the life cycle of the IS, a configuration management plan shall be in place for security-relevant hardware, firmware, and software.
- c. Program Managers (PMs), IAOs, and SAs maintain control of changes to the formal model as documented in the SSAA.
- d. Tools shall be available and maintained under strict configuration control for comparing a newly generated version of software with the previous version. These tools must ascertain that only the intended changes have been made in the code that will be used as the new version of the IS.
- e. Documentation of hardware and software configurations and diagrams shall be established and maintained to allow resumption of operations after a hardware/software failure.

3.7 Contract Management – MHS guidance requires that IA requirements be properly reflected in all MHS contracts awarded for the provision of IT products and services.

3.7.1 All MHS contracts for the provision of IA and IA-enabled products or services shall include a restriction to use only properly evaluated and validated products, as required by DoDD 8500.1 “Information Assurance,” (reference a.).

3.7.2 All MHS contracts for the provision of IA and IA-enabled products or services shall include requirements for protection of DoD SI and shall be monitored for compliance.

3.7.3 MHS contracts for IA services shall include a statement that selected labor categories in RFPs or SOWs may be designated Information Technology (IT) sensitive positions or national security positions. Contractor personnel who will need access to unclassified information systems may be assigned to one of three position sensitivity designations: Automated Data Processing (ADP)-I (Privileged), ADP-II (Limited Privileged) and ADP-III (Non-Privileged). Contractor personnel requiring access to sensitive or classified information must have or be capable of obtaining a favorable adjudication of an investigation into their background.

3.7.4 MHS outsourced healthcare administrative support services (ancillary administrative services such as home-based transcription) that require transfer, storing, or processing of patient sensitive information must meet the same health data protection standards as expected within the medical treatment facility. Contract requirements will outline protective measures and staff training requirements to ensure patient sensitive information is protected appropriately.

3.8 Incident Reporting and Response

3.8.1 TMA Components shall have a comprehensive process to audit, detect, isolate, and react to intrusions, service disruptions, and incidents that threaten the security of operations.

3.8.2 Reporting and Response

- a. TMA Components shall report incidents in accordance with pre-established escalation procedures for the affected IS. The Joint Task Force, Computer Network Operations (JTF CNO) provides assistance in identifying, assessing, containing, and countering incidents that threaten DOD ISs.
- b. All users shall immediately report all suspected or confirmed virus, worm, and malicious logic instances to their Help Desk.

3.9 Security Awareness, Training, and Education.

3.9.1 All MHS personnel shall be informed of applicable organizational policies and procedures concerning DOD ISs and shall be expected to act effectively to ensure the security of system resources. Initial and annual user security training and awareness will ensure all users are aware of security issues and what actions to take when an event or incident occurs.

3.9.2 An IA security training and awareness program shall be maintained for all MHS personnel.

- a. All users shall be required to undergo security training upon initial assignment. Thereafter, individuals must receive annual refresher training to assure they continue to understand and abide by MHS policies and procedures governing IA.
- b. Training shall be tailored to information the user needs to know to operate the IS securely.
- c. Personnel with security-specific responsibilities will require additional specialized training.

3.10 Physical Security

3.10.1 DoD 5200.8-R, "Physical Security Program" (reference j.) provides guidelines to be used by federal organizations in structuring physical security programs.

3.10.2 Facility management shall develop physical security plans that incorporate IS physical security.

3.10.3 Physical security shall be continually enforced, annually evaluated, and updated as required.

3.11 Personnel Security

3.11.1 All TMA Components shall operate and maintain a Personnel Security Program in accordance with DoD 5200.2-R, "Personnel Security Program" (reference i.) A level of trustworthiness shall be established before personnel are granted access to DoD ISs or DoD sensitive information. DoD requires all DoD military and civilian personnel, contractor employees, consultants, and other designated persons affiliated with the DoD who manage, design, develop, operate, or access a DoD IS or process DoD information, to undergo an appropriate background investigation and security awareness training before access is granted to an IS or DoD information.

3.11.2 Separation of Duties - Roles and responsibilities shall be separated in accordance with Office of Management and Budget (OMB) Circular A-130, "Management of Federal Information Resources" (reference w.) which requires that key duties and responsibilities in authorizing, processing, recording, and reviewing official transactions are separated among individuals, and that managers exercise appropriate oversight to ensure that individuals do not exceed or abuse their assigned authorities. The MHS IA Program Office requires that roles and responsibilities be separated to avoid any conflict of interest.

3.11.3 Employee Behavior

- a. DoD 5500.7-R, "Joint Ethics Regulation" (reference k.) establishes federal ethics for use of government resources to include use of the Internet. The MHS may provide civilian employees and assigned military personnel, temporary workers, independent contractors, and agents access to the Internet to perform assigned business functions. Individuals shall be notified of their privacy rights and security responsibilities when attempting access to DOD ISs.
- b. Internet/E-mail Ethics:
 - Internet/e-mail systems and commercial systems paid for by the federal government shall be for official use and authorized purposes only except as noted in DoD 5500.7-R, "Joint Ethics Regulation" (reference k.).
 - Official use includes emergency communications and communications that are necessary in the interest of the federal government.
 - Incidents of unauthorized activity or misuse or abuse of the Internet or e-mail use will be investigated and the perpetrator shall be subject to disciplinary action and/or monitoring action as appropriate.
 - MHS personnel shall not transmit SI or PHI via the Internet/e-mail or other electronic means unless appropriate security controls (e.g., encryption, Public Key Infrastructure (PKI)) are in place.

3.12 Identification and Authentication

- 3.12.1 User identification and password systems support the minimum requirements of accountability, access control, least privilege, and data integrity. DoD IS users shall be granted access only to the resources they need to perform their official functions. The features and practices described in Computer Security Center Standard CSC-STD-002-85, "Department of Defense Password Management Guideline," (reference m.) shall be incorporated into DoD ISs.
- 3.12.2 Password Management – DoD IS access is gained through the presentation of an individual identifier and password. For DoD ISs utilizing a logon identification (ID) as the individual identifier, the IAO, SA, and user shall ensure passwords, at a minimum, meet the requirements identified in CSC-STD-002-85, "Department of Defense Password Management Guideline" (reference n.).
- 3.12.3 Public Key Infrastructure – The use of PKI is a method to achieve non-repudiation by which the sender of information is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the information. The use of PKI certificates for authentication of a user's or systems identity shall be in accordance with published DoD policy and procedures (references n., o., and p.). These technologies shall be incorporated in systems containing SI or PHI. Where interoperable PKI is required for the exchange of unclassified information with vendors and contractors, the MHS shall only accept PKI certificates obtained from a DoD-approved external certificate authority or other mechanisms approved in accordance with DoD policy.

3.13 Audit Logs and Review

- 3.13.1 Audit Logging – The system must record all transactions, updates, changes, and accesses to DoD ISs in audit logs. The system must create and maintain an audit trail so actions affecting the system can be traced back to the responsible party based on individual identity. The system must also protect the audit information from modification or unauthorized access or destruction.
- 3.13.2 Audit Review - Audit records for DoD ISs shall be reviewed by the MHS IA Program Office during the C&A process. Individual sites shall review audit records for DoD ISs on a monthly basis or more frequently when deemed necessary. In those cases where an intrusion or other unauthorized act may have taken place, the audit logs shall be secured and reviewed as soon as possible by the appropriate authorities. Optimum use shall be made of data reduction or other automated audit log management tools.

3.14 Data Integrity

- 3.14.1 Safeguards shall be implemented to detect and minimize inadvertent modification or destruction of data, and to detect and prevent malicious destruction or modification of data.
- 3.14.2 Virus protection shall be installed, enabled, and maintained on all DoD ISs.

3.14.3 Security monitoring shall occur within each TMA Component. The IS owners shall ensure the ISs under their purview are regularly monitored, system records are reviewed on a weekly basis, and that all DoD ISs are protected by Intrusion Detection Systems (IDS).

3.15 Production, Input, and Output Controls

3.15.1 Production controls used for the marking, handling, processing, storage, and disposal of input and output information and media, as well as labeling and distribution procedures shall be placed on MHS information and media to include printers, fax machines, copiers and biomedical devices (DoD 5200.1-R, "Information Security Program" (reference h.)). Production controls shall be identified during the requirements phase of the system life cycle management or acquisition process.

3.15.2 Sensitive information (SI) is information, whose loss, misuse, or unauthorized access to or modification could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled. All output shall be marked to accurately reflect the sensitivity of the information. The marking may be automated (e.g., the IS has a feature that produces the markings) or may be done manually. When SI information is included in DoD documents, it shall be marked as if the information were For Official Use Only as defined in Title 17, United States Code, Section 106, "Copyrights" (reference y.).

3.15.3 Electronic Storage Media/Equipment Disposition - Sanitization, documentation, labeling and disposition of all unclassified electronic storage media/equipment shall be accomplished consistent with DoD requirements. Proper sanitization of electronic storage media/equipment that has been used for patient sensitive information is vitally important to the MHS and must follow DoD guidelines as outlined below. In addition, sanitization documentation must be maintained for a minimum of six years to ensure compliance with HIPAA security requirements.

Electronic storage media/equipment under vendor warranty or maintenance contract do not have to be sanitized prior to transfer from government control to the vendor/contractor. Maintenance contracts should be written to affirm the protection of the DoD information and especially patient sensitive information by the contractor/vendor. If the electronic storage media/equipment is to be disposed of outside of government control, the information owner must use the approved methods and procedures found in Assistant Secretary of Defense (Command, Control, Communications, and Intelligence) Memorandum, "Disposition of Unclassified DoD Computer Hard Drives," June 4, 2001 and accompanying attachments. Although the memorandum deals primarily with DoD computer hard drives, MHS guidance dictates disposition of all electronic storage media in accordance with the above memorandum.

The term "electronic technology storage media/equipment" as used herein means any permanent or semi permanent electronic storage technology including, but not limited to: hard drive storage devices used in computers or biomedical equipment,

back-up tapes, and removable magnetic or optical media and electronic computer equipment.

3.16 Software Usage

- 3.16.1 Regardless of the mission assurance category or confidentiality level of the MHS information system, all incorporated IA products and IA-enabled products that require use of the product's IA capabilities, acquired under contracts executed after July 1, 2002, shall comply with the evaluation and validation requirements of NSTISSP No. 11 (reference t.). Qualifications and other considerations may be found in paragraph E.3.2.5, DoDI 8500.2, "Information Assurance Implementation" (reference b.).
- 3.16.2 MHS activities with a mission-related requirement for installing other than government purchased software must obtain a waiver from the IAO with approval from the appropriate DAA.
- 3.16.3 Users shall abide by Section 106 of Title 17, United States (U.S.) Code, "Copyrights" (reference y.), which gives copyright owners exclusive rights to reproduce and distribute their material.
- 3.16.4 Copyrighted software products are not to be reproduced except to the limit provided by contract (e.g., archive copy for backup).

3.17 Wireless IT

- 3.17.1 When incorporating wireless services, devices, and technological implementations within the TMA Components, it shall be in accordance with DoDD 8500.1, "Information Assurance (IA)" (reference a.). In that wireless technology (e.g., infrared, acoustic, radio frequency) can store, process, and/or transmit information outside the physical confines of the MHS and introduces additional vulnerabilities, they shall not be connected to MHS systems without the approval of the appropriate DAA.
- 3.17.2 Classified information shall not be stored, processed, and/or transmitted on MHS wireless devices.
- 3.17.3 Only wireless devices that are procured, configured, maintained, and owned by the government shall interface with DoD ISs.
- 3.17.4 Wireless devices shall incorporate the provisions of NIST and DISA guidelines for incorporating security settings.

4 GUIDANCE CHANGE DEVELOPMENT

- 4.1 Responsibility for implementing changes to this guidance rests with the MHS IA Program Office or the MHS Chief Information Officer (CIO). The following process integrates the

valuable input and contribution of several groups including each Service, the Program Executive Officer/Joint Medical Information Systems Office (PEO/JMISO), the Information Assurance Working Group (IAWG), the Technical Integration Working Group (TIWG), and the MHS Enterprise Architecture Board (EAB).

4.1.1 When new DoD or applicable national level guidance, such as federal regulations or public laws, are promulgated or changes to existing IA policies occur, the MHS IA Program Office shall assess their impact on this guidance. The IAWG will propose and present changes to modify, include, or exclude specific sections of this Guidance.

4.1.2 It is the responsibility of the Service representatives to the IAWG to review new Service policies or updates to published Service policies and assess their impact on this Guidance. The Service representatives to the IAWG will propose and present changes to modify, include, or exclude specific sections of this Guidance. These suggestions will be assessed by the MHS IA Program Office and presented to the IAWG voting members for information, comment, and proposed alternative resolutions within 60 days of submission.

4.2 Guidance Change Process:

4.2.1 When new guidance or a change to existing policy is required, the IAWG's representative or the IA Program Office will develop a draft of the proposed change.

4.2.2 IAWG members (this includes TIWG review and comment) will be presented with proposed IA guidance or policy changes for review, comment, and concurrence.

4.2.3 After IAWG coordination and concurrence, the draft guidance will be provided to the EAB for review and comment.

4.2.4 The draft guidance will then be briefed to the MHS CIO to request approval for presentation of the draft guidance to the Information Management Program Review Board.

4.2.5 Once the IAWG has presented the draft guidance to the PRB and has received approval, the accepted guidance is forwarded through the MHS CIO to the Assistant Secretary of Defense (health Affairs) for signature.

4.2.6 The signed guidance will be promulgated for implementation throughout the MHS to include the Service Medical Departments, MHS Joint Medical Information Systems Office, TMA directorates, and MHS contractors.

5 ROLES AND RESPONSIBILITIES

5.1 One of the most important elements of the MHS IA Program is ensuring that personnel are aware of their roles and responsibilities in maintaining the security of the DoD ISs, as well as all sensitive information. Personnel who manage, design, develop, program, operate, or

use DoD ISs have responsibilities that contribute toward the success of the MHS IA Program. IA functions may be performed full time by an employee in an IT position, or part time by an employee in a designated IA role as a collateral or adjunct duty. The position titles utilized in this guidance reflect MHS nomenclature, but it is acceptable for MHS Contractors to have personnel with equivalent responsibilities and position titles fulfilling these requirements.

5.2 Head of DoD Component shall:

5.2.1 Assign mission assurance categories for DoD Component-specific DoD information systems according to the guidelines provided in and DoDI 8500.2, "Information Assurance Implementation," (reference b.).

5.2.2 Appoint Designated Accrediting Authorities in accordance with DoDD 8500.1, "Information Assurance," and DoDI 8500.2, "Information Assurance Implementation," (reference a. and b.).

5.2.3 Disseminate MHS IA guidance to the TMA and Service Surgeons General.

5.3 Service Surgeons General shall:

5.3.1 Ensure the development and implementation of a Service medical department IA program.

5.3.2 Initially report IA compliance biannually to the Assistant Secretary of Defense (Health Affairs) then report annually once the MHS IA Program matures.

5.3.3 Distribute MHS IA guidance to MTF commanders.

5.4 The MHS Chief Information Officer (CIO) shall:

5.4.1 Fulfill the role of the MHS senior official responsible for the development, implementation, maintenance, and oversight of the MHS IA program. In this capacity, the MHS CIO shall provide strategic and tactical program direction, allocate necessary program resources, and exercise authority over all programmatic components as necessary to accomplish MHS IA goals and objectives.

5.4.2 Ensure that IA is integrated into all policies and procedures used to plan, procure, develop, implement, and manage the MHS infrastructure and ISs.

5.4.3 Ensure that IA is integrated into the MHS enterprise architecture.

5.4.4 Formally appoint an IA Program Manager in accordance with DoDD 8500.1, "Information Assurance (IA)" (reference a.).

5.4.5 Define strategic IA goals, annual objectives, and ensure that such goals and objectives are funded and tracked.

- 5.4.6 Delegate responsibilities for program implementation to Component heads as appropriate.
- 5.5 The MHS IA Program Manager shall:
 - 5.5.1 Establish, manage, and assess the effectiveness of the MHS IA Program.
 - 5.5.2 Develop and promulgate IA Guidance.
 - 5.5.3 Ensure Risk and Vulnerability Assessments are accomplished for all DoD ISs with Service-specific ISs being the responsibility of the Service CIOs.
 - 5.5.4 Provide C&A services.
 - 5.5.5 Provide IA architecture support.
 - 5.5.6 Ensure security awareness, education, and training are conducted.
 - 5.5.7 Manage the Information Assurance Vulnerability Management (IAVM) program.
 - 5.5.8 Be formally appointed in writing.
- 5.6 Designated Accrediting Authority (DAA)
 - 5.6.1 MHS DAAs are formally appointed and assigned in writing by the Assistant Secretary of Defense (Health Affairs) (ASD(HA)). A DAA shall be formally appointed in writing for each DoD IS operating within or on behalf of the MHS, to include outsourced business processes supported by private sector ISs and outsourced information technologies. The DAA shall be a U.S. citizen, a DoD employee, and possess the level of authority required to formally accept the risk for operating DoD ISs under his/her purview.
 - 5.6.2 DAAs shall:
 - a. Review and formally approve DoD IS security safeguards, and issue accreditation statements that are based upon the acceptability of the security safeguards and associated level residual risk for each IS under his or her purview.
 - b. Grant an Authorization To Operate (ATO) for DoD ISs meeting MHS IA requirements.
 - c. Grant an Interim Authorization to Operate (IATO) for DoD ISs meeting DIACAP requirements for an IATO. The IATO shall not exceed a 12-month period during which all security issues required to meet an ATO accreditation shall be satisfactorily resolved.
 - d. Ensure ISs under development are accredited prior to deployment. Identify security deficiencies and, where the deficiencies are sufficiently serious to preclude accreditation, take appropriate action to achieve an acceptable security level.

- e. Establish and verify for each IS under his/her purview data ownership, accountability, access rights, and special handling requirements.
- f. Verify that an appropriate mission assurance category has been assigned for each IS under his/her purview.
- g. Ensure that IAMs, IAOs, and SAs are formally designated and assigned in writing for all ISs under his/her purview, and that they receive the level of training and appropriate certifications necessary to perform the tasks associated with assigned responsibilities.
- h. Ensure a process for managing information security incidents that includes prevention, detection, response, and lessons learned is developed, implemented and maintained for all ISs under his/her purview.
- i. Ensure continuous life-cycle oversight and surveillance of the security safeguards approved during the C&A process through establishment of surveillance plans, performance metrics and reporting procedures to monitor information assurance compliance with guidance.
- j. Ensure a security education, awareness, and training program that addresses all MHS personnel categories, to include general users, IT professionals, managers, and senior executives is developed, implemented, and maintained for all ISs under his/her purview.
- k. Ensure that documented Memorandums of Agreement (MOAs) to address security requirements are in place for all ISs under his/her purview that interface or are networked, and managed by different DAAs.
- l. Ensure that documented MOAs to address security requirements are in place for all ISs under his/her purview that interface or are networked to non-DoD entities.
- m. Ensure the reaccreditation of ISs under his/her purview at least every three years, or more frequently if deemed necessary due to major IS modifications or like modifications to the operating environment.
- n. Formally appoint and assign in writing Designated Accrediting Authority Representatives (DAARs) and Certifiers for select ISs under his/her purview, as deemed appropriate. The DAAR has the same responsibilities as the DAA, can approve an initial IATO, and will ensure that any and all subsequent IATO requests are forwarded to the appropriate DAA for review and approval.

5.7 Certifier

5.7.1 The Certifier (or Certifying Authority – “Interim Department of Defense Certification and Accreditation Process (DIACAP) Guidance,” (reference c.) for a given DoD IS is designated by the appropriate DAA for that IS with the authority to establish and manage the organization’s C&A process and to verify and validate IS security design and implementation through testing and review of IS security documentation.

5.7.2 The Certifier shall:

- a. Ensure a comprehensive, standardized risk analysis and security evaluation is completed prior to IS certification.
- b. Certify the extent to which ISs meet prescribed security requirements.
- c. Prepare the IS C&A report and forward the complete report with recommendations on accreditation to the appropriate DAA.
- d. Maintain and provide other records and reports of C&A activities, as necessary.

5.8 Program Executive Officer (PEO)/Joint Medical Information Systems (JMIS) Office

DoDI 5000.2, "Operation of the Defense Acquisition System," (reference f.) identifies the PEO as a military or civilian official who has primary responsibility for directing several major defense acquisition programs and for assigned major system and non-major system acquisition programs.

5.8.1 The PEO JMIS is responsible for implementation of IA requirements for the ISs under his/her purview.

5.8.2 The PEO JMIS is responsible for the supervision and senior management of all JMIS PMs and provides guidance, direction, and oversight to those PMs.

5.8.3 JMIS Program Managers shall:

- a. Maintain responsibility for the security posture of all ISs and data under his/her purview.
- b. Work closely with the IA Program Manager in administering the MHS IA Program.
- c. Ensure all required resources, to include funding and personnel, are appropriately budgeted and available to implement and maintain required C&A security safeguards.
- d. Ensure the development and implementation of a C&A Plan for each IS under his/her purview.
- e. Ensure the participation of IS security personnel early in the IS development life cycle to assist in the identification and selection of appropriate security controls, and provide guidance on the accreditation process.
- f. Author all required MOAs to address security requirements between: ISs that interface, ISs that are networked and are managed by different DAAs, or ISs networked to non-DoD entities.
- g. Verify the design of IS security for systems under his/her purview.
- h. Verify the implementation of security design in the developed IS by ensuring thorough security testing is performed.
- i. Initiate protective or corrective measures immediately upon identification of security weaknesses/issues.
- j. Take all necessary and appropriate measures to resolve outstanding IS security deficiencies in a timely manner to establish a level of security necessary to achieve accreditation.
- k. Ensure that required security controls are properly implemented and maintained throughout the life-cycle of all ISs under his/her purview.

- l. Ensure that the appropriate functional managers have properly identified and classified the data processed, stored, and/or transmitted by all the ISs under his/her purview.
- m. Ensure that quality assurance reviews are performed routinely to minimize the risk of errors and preserve IS and data integrity for all ISs under his/her purview.
- n. Monitor all contractors under his/her purview with access to DOD ISs to ensure compliance with this and all other referenced policies and procedures.
- o. Provide assistance, as needed, to security personnel during the accreditation and reaccreditation processes.
- p. Ensure compliance with the MHS IAVM Program.

From time to time, MHS may invite the Surgeons General of the Department of the Army, Air Force, and Navy to send one or more Military Department (MILDEP) representatives to sit on Working Groups or act as liaison to the Joint Medical Information Systems Office/Program Offices. Program Managers for developing and fielded MHS Joint/Program of Record systems that run on networks under control of the Services, or pass through networks under control of the Services, shall involve and begin a dialogue, in the requirements phase of a system's development or its update, with appropriate Military Department (MILDEP) representatives to MHS.

Program Managers shall ensure information is passed to appropriate MILDEP representatives during DIACAP development and as certification and re-certification events take place. The information shall be in a format so that the Service Certifying Authority/Certifier can evaluate the technologies proposed, such as ports, protocols, and services (PPS), use of mobile code, VPNs, wireless, etc., that PMs are considering for use in their new or upgraded system or application. This dialogue will help identify potential conflicts with Service policy and allow ample time to resolve them. This is especially true if the technologies being considered for use are new.

Prior to installation of any new MHS Joint/POR system, or upgrade/reconfiguration to an existing legacy system, the system's PM shall provide the Military Department (MILDEP) representatives with the following:

- A copy of the system's DIACAP documentation
- A copy of the MHS CA/Certifier's assessment of the system's residual or remainder risks
- A formal "Type" Accreditation decision, either Interim or Final Authorization to Operate (IATO or ATO).

It is the intent of MHS that the Military Department (MILDEP) representative shall convey this documentation to the Service CA/Certifier. These documents will permit the Service CA/Certifier to make informed decisions regarding operation of new/upgraded/reconfigured systems on their network(s), the incorporation of systems into their network Certification and Accreditation package(s), and granting/continuing an appropriate IATO or ATO for their network(s).

5.9 Information Assurance Manager (IAM)

5.9.1 The IAM serves as the focal point for policy guidance on IA matters pertaining to ISs under his/her purview. In addition to the roles and responsibilities outlined in DoDI 8500.2, "Information Assurance (IA) Implementation" (reference b.), IAMs shall:

- a. Provide IA policy and program guidance to subordinate activities.
- b. Maintain overall responsibility for the IA Program within his/her activity by establishing, managing, and assessing the effectiveness of the program.
- c. Ensure compliance with approved MHS IA policies and procedures.
- d. Ensure that compliance monitoring of ISs under his/her purview occurs, and review the results of such monitoring.
- e. Ensure that IA inspections, tests, and reviews are coordinated within his/her activity.
- f. Ensure that all IA management review items are tracked and reported.
- g. Complete job-specific IA training on an annual basis.

5.10 Military Treatment Facility Commanders shall:

5.10.1 Ensure MHS IA guidance implementation.

5.10.2 Provide MHS IA compliance information to their respective Surgeons General.

5.11 Information Assurance Officers (IAO)

5.11.1 The IAO ensures that the systems under his/her purview are operated and maintained at the appropriate level of security, oversees the implementation of all applicable IS security requirements, and monitors IS security operations. In addition to the roles and responsibilities identified in DoDI 8500.2, "Information Assurance (IA) Implementation" (reference b.), IAOs shall:

- a. Act in the capacity of IA expert for ISs under his/her purview, and as such shall be responsible for coordinating IA issues with the MHS IA Program Office. The IAO also serves as an IA advisor to the Certifier, the IAM, and the DAA.
- b. Ensure that ISs are operated, used, maintained, and disposed of in accordance with all applicable IA policies and procedures.
- c. Enforce IA policies and safeguards for all personnel afforded access to the IS for which the IAO has cognizance.
- d. Comply with DoD 5200.2-R, "Personnel Security Program" (reference i.) governing personnel security clearances and the designation of automated data processing (ADP)/IT positions and security investigation requirements.
- e. Ensure that users have the required authorization and need-to-know, have been indoctrinated, and are familiar with internal security practices before being granted access to the IS.
- f. Prepare a C&A Plan for ISs under his/her purview.

- g. Ensure IS security safeguards required for all ISs under his/her purview are addressed in the IS documentation.
- h. Review audit trails for all ISs under his/her purview at least weekly or more frequently if deemed necessary.
- i. Report incidents to the DAA and the DoD reporting chain, as required, and coordinate responses to IA-related alerts.
- j. Develop and provide reports on the IA posture of all ISs under his/her purview as required by the DAA.
- k. Ensure that security procedures and protocols governing IS operations are developed, promulgated, and maintained for ISs.
- l. Ensure consistent progress toward site accreditation of all ISs under his/her purview.
- m. Ensure adherence to IAVM procedures and processes.
- n. Ensure the development, maintenance, and annual testing of required contingency plans.
- o. Ensure individual access to a particular DOD IS is revoked immediately upon determination that such access is no longer required (e.g., completion of project, transfer, retirement, resignation).
- p. Complete job-specific IA training on an annual basis.

5.12 Privileged Users (e.g., System Administrators, Network Security Officer)

5.12.1 Privileged Users meet all MHS requirements for authorized users. Privileged Users shall:

- a. Ensure servers, workstations, peripherals, communication devices, application software, and all other applicable IT assets are available to support users.
- b. Ensure approved anti-virus software is installed, maintained, and updated on all servers and workstations under his/her purview.
- c. Assist the IAO in maintaining IS configuration controls and access levels consistent with the need-to-know doctrine.
- d. Advise the IAO of security anomalies or integrity deficiencies immediately upon detection.
- e. Administer user identification or authentication mechanisms of all ISs under his/her purview.
- f. Perform system backups, software upgrades, and system recovery, including the secure storage and distribution of backups and upgrades.
- g. Coordinate with the IAO, as required, to enforce password controls, set permissions, perform security management functions, and coordinate and/or perform IS preventative and corrective maintenance problems. Document and report any identified vulnerabilities to the IAO immediately upon detection.
- h. Report to the IAO all IS failures that could lead to unauthorized disclosure or any attempt to gain unauthorized access to DoD ISs and/or data processed, stored and/or transmitted by the IS.
- i. Configure and monitor the IDS.
- j. Coordinate Help Desk support as required.
- k. Complete job-specific IA training on an annual basis.

5.13 Authorized Users shall:

- a. Observe all applicable IA policies, regulations, procedures, and practices governing the secure operation (e.g., protection of passwords) and authorized use of ISs.
- b. Report all security incidents, potential threats, and suspected vulnerabilities to the appropriate IAO or IAM immediately upon detection.
- c. Complete initial and annual security awareness training.
- d. Possess the appropriate credentials (e.g., Background Investigations, Security Clearances) required for general and/or privileged levels of access to DoD ISs.
- e. Access only that data, software, hardware, and firmware for which they are authorized access and have a need-to-know, and assume only authorized roles and privileges.
- f. Protect all IS access authenticators, such as individual IDs and Passwords, commensurate with the classification or sensitivity of the information accessed. Immediately report any compromise or suspected compromise of an authenticator to the appropriate IAO immediately upon detection.
- g. Ensure that IS media and output are properly marked, controlled, stored, transported, and destroyed in accordance with the classification or sensitivity and need-to-know.
- h. Protect terminals or workstations from unauthorized access.
- i. Immediately inform the IAO when access to a particular DoD IS is no longer required (e.g., completion of project, transfer, retirement, resignation).
- j. Observe policies and procedures governing the secure operation and authorized use of any DoD IS to which they have been granted access.
- k. Use the DoD IS only for authorized purposes.
- l. Not unilaterally bypass, strain, or test IA mechanisms. If IA mechanisms must be bypassed, users shall coordinate the procedure with the IAO and receive written approval from the IAM.
- m. Not introduce or use unauthorized software, firmware, or hardware on the DoD IS. Users shall not relocate or in any way change, or cause to change, DoD IS equipment or the network connectivity of equipment without proper IAM authorization.

6 EFFECTIVE DATE

This Guidance is effective immediately.

Enclosures – 3

E-1: References

E-2: Definitions

E-3: Acronyms

ENCLOSURE 1

REFERENCES

- e. DoDD 5000.1, "The Defense Acquisition System," 12 May 2003
- f. DoDI 5000.2, "Operation of the Defense Acquisition System," 12 May 2003
- g. DoDI 8580.1, "Information Assurance (IA) In the Defense Acquisition System," 9 July 2004
- h. DoD 5200.1-R, "Information Security Program," January 1997
- i. DoD 5200.2-R, "Personnel Security Program," Change 3, 23 February 1996
- j. DoD 5200.8-R, "Physical Security Program," May 1991
- k. DoD 5500.7-R, "Joint Ethics Regulation," Change 6, 23 February 2006
- l. Assistant Secretary of Defense Memorandum, subject: "Public Key Infrastructure (PKI) Policy Update," 21 May 2002
- m. Computer Security Center Standard, CSC-STD-002-85, "Department of Defense Password Management Guideline," 12 April 1985
- n. DoD Chief Information Officer Memorandum, subject: "Public Key Enabling (PKE) of Applications, Web Servers, and Networks for the Department of Defense (DoD)," 17 May 2001
- o. DoD Chief Information Officer Memorandum, subject: "Common Access Card," 16 January 2001
- p. DoD PKI Program Management Office Memorandum, subject: "X.509 Certificate Policy for the United States Department of Defense," 9 February 2005
- q. Freedom of Information Act of 1986 (Public Law 99-570)
- r. Military Handbook (MIL-HDBK) 61A, "Configuration Management Guidance," February 7, 2001
- s. National Computer Security Center – Technical Guidance (TG)-006, "A Guide to Understanding Configuration Management in Trusted Systems," 16 October 2002
- t. National Security Telecommunications and Information Systems Security Policy (NSTISSP) No. 11, National Policy Governing the Acquisition of Information Assurance (IA) and IA-Enabled Information Technology (IT) Products, issued January 2000, revised June 2003
- u. NIST, Special Publication 800-34, "Contingency Planning Guide for Information Technology Systems," June 2002
- v. Office of the Secretary of Defense Memorandum, subject: "Common Access Card – Changes," 18 April 2002
- w. OMB Circular No. A-130, "Management of Federal Information Resources," Appendix III, "Security of Federal Automated Information Systems," 30 November 2000
- x. Privacy Act of 1974 (Public Law 93-579), Title 5 U.S. Code, Section 552a
- y. Title 17, United States Code, Section 106, "Copyrights"

ENCLOSURE 2

DEFINITIONS

Access – A specific type of interaction between a subject and an object resulting in the flow of information from one to the other.

Accountability – The property that enables activities on a system to be traced to individuals who may then be held responsible for their actions.

Accreditation – A formal declaration by the DAA that the IS is to operate in a particular security mode using a prescribed set of safeguards. Accreditation is the official management authorization for operation of ISs on the certification process as well as other management considerations. The accreditation statement affixes security responsibility with the DAA and shows that due care has been taken for security.

Assurance – A measure of confidence that the security features and architecture of an IS accurately mediate and enforce the security policy.

Audit Trail – A chronological record of system activities sufficient to enable the reconstruction, reviewing, and examination of the sequence of environments and activities surrounding or leading to an operation, a procedure, or an event in a transaction from its inception to final results.

Authenticators - Security measures such as individual account identification and passwords that are designed to verify an individual's authorization to access a system or receive specific categories of information.

Authorization – The granting of access rights to a user, program, or process by a responsible administrator.

Authorization to Operate (ATO) – The authorization, granted by a DAA, for a DoD information system to process, store, or transmit information. Authorization is based on acceptability of the IA component, the system architecture, and implementation of assigned IA controls.

Backup – A copy of data and/or applications contained in the IS stored on magnetic media outside of the IS to be used in the event IS data is lost.

Certification – A comprehensive validation of actual IA capabilities and services of a DoD information system, made as part of and in support of the DIACAP, to establish compliance with assigned IA controls based on standardized procedures.

Compromise – A violation of the security policy of a system such that unauthorized disclosure of SI may have occurred.

Confidentiality – Assurance that information is not disclosed to unauthorized persons, processes, or devices.

Configuration Control –(1) A systematic process that ensures that changes to released configuration documentation are properly identified, documented, evaluated for impact, approved by an appropriate level of authority, incorporated, and verified. (2) The configuration management activity concerning: the systematic proposal, justification, evaluation, coordination, and disposition of proposed changes; and the implementation of all approved and released changes into (a) the applicable configurations of a product, (b) associated product information, and (c) supporting and interfacing products and their associated product information.

Configuration Management – A management process for establishing and maintaining consistency of a product’s performance, functional, and physical attributes with its requirements, design, and operational information throughout its life.

Contingency Plan – A plan for emergency response, backup operations, and post-disaster recovery maintained by an activity as a part of its security program that will ensure the availability of critical resources and facilitate the continuity of operations in an emergency situation.

Continuity of Operations Plan – A plan for developing advanced arrangements to stand up critical operations following an unplanned event that disrupts critical operational processes.

Countermeasure – Any action, device, procedure, technique, or other measure that reduces the vulnerability of or threat to a system.

Data – A representation of facts, concepts, information, or instructions suitable for communication, interpretation, or processing by users or by an IS.

Defense-in-Depth – The security approach whereby layers of IA solutions are used to establish an adequate IA posture. Implementation of this strategy also recognizes that due to the highly interactive nature of the various systems and networks, IA solutions must be considered within the context of the shared risk environment and that any single system cannot be adequately secured unless all interconnected systems are adequately secured.

Designated Accrediting Authority – The official who has the authority to decide on accepting the security safeguards prescribed for an IS or that official who may be responsible for issuing an accreditation statement that records the decision to accept those safeguards.

DIACAP Package – The collection of documents or collection of data objects generated through DIACAP implementation for an information system. A DIACAP package is developed through implementing the activities of the DIACAP and maintained throughout a system’s life cycle. Information from the package is made available as needed to support an accreditation or other decision such as a connection approval. There are two types of DIACAP packages, the Comprehensive Package containing all information connected with the certification of the information system, and the Executive Package containing minimum information for an accreditation decision. The Comprehensive package contains the System Identification Profile (SIP), the DIACAP Implementation Plan, the Certification Documentation, the DIACAP Scorecard, and the POA&M if required. The Executive package contains the System Identification Profile, the DIACAP Scorecard, and the POA&M if required.

DoD Information Assurance Certification and Accreditation Process (DIACAP) –

The DoD processes for identifying, implementing, validating, certifying, and managing IA capabilities and services, expressed as IA Controls, and authorizing the operation of DoD information systems in accordance with statutory, federal and DoD requirements.

Disaster Recovery Plan – A plan for developing advance arrangements and procedures that will enable an organization to respond to a disaster and resume its critical business operations within a predetermined period of time, minimize the amount of loss, and repair the stricken facilities as soon as possible.

Enclave - Collection of computing environments connected by one or more internal networks under the control of a single authority and security policy, including personnel and physical security. Enclaves always assume the highest mission assurance category and security classification of the AIS applications or outsourced IT-based processes they support, and derive their security needs from those systems. They 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 OMB Circular No. A-130, “Management of Federal Information Resources” (reference w.). Enclaves may be specific to an organization or a mission, and the computing environments 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.

Identification – The process that enables recognition of an entity by a system, generally by the use of unique machine-readable user names.

Information Assurance – Information operations that protect and defend information and information systems by ensuring their availability, integrity, authentication, confidentiality, and non-repudiation.

Information Assurance Manager (IAM) – The individual responsible for the IA program of a DoD information system or organization. While the term IAM is favored within the DoD, it may be used interchangeably with the title Information Systems Security Manager (ISSM).

Information Assurance Officer – An individual responsible to the IAM for ensuring that the appropriate operational IA posture is maintained for a DoD information system or organization.

Information Assurance Vulnerability Alert – Comprehensive distribution process for notification of Combatant Commanders, Services, and Agencies about vulnerability alerts and countermeasures information.

Information System – A set of information resources organized for the collection, storage, processing, maintenance, use, sharing, dissemination, disposition, display, or transmission of information. Includes AIS applications, enclaves, outsourced IT-based processes, and platform IT interconnections.

Integrity – Quality of an IT system reflecting the logical correctness and reliability of the operating system; the logical completeness of the hardware and software implementing the

protection mechanisms; and the consistency of the information structures and occurrence of the stored information. It is composed of data integrity and system integrity.

Interim Authorization to Operate – Temporary authorization to operate a DoD IS under the conditions or constraints enumerated in the accreditation decision.

Need-To-Know – The necessity for access to, knowledge of, or possession of specific information required to carry out official duties.

Network – A network is composed of a communications medium and all components attached to that medium whose responsibility is the transference of information.

Non-repudiation – The method by which the sender of information is provided with proof of delivery and the recipient is assured of the sender's identity so that neither can later deny having processed the information

Outsourced IT-based Process - For DoD IA purposes, an outsourced IT-based process is a general term used to refer to outsourced business processes supported by private sector information systems, outsourced information technologies, or outsourced information services. An outsourced IT-based process performs clearly defined functions for which there are readily identifiable security considerations and needs that are addressed in both acquisition and operations.

Password – A protected, private character string used to authenticate an identity.

Penetration Testing – The portion of security testing in which the evaluators attempt to circumvent the security features of a system. The evaluators may be assumed to use all system design and implementation documentation, which may include listings of system source code, manuals, and circuit diagrams. The evaluator's work under the same constraints applied to ordinary users.

Personnel Security – The procedures established to ensure that all personnel who have access to sensitive information have the required authority, as well as appropriate clearances.

Physical Security – The application of physical barriers and control procedures as preventive measures or countermeasures against threats to resources and sensitive information.

Platform IT Interconnection - For DoD IA purposes, platform IT interconnection refers to network access to platform IT. Platform IT interconnection has readily identifiable security considerations and needs that must be addressed in both acquisition and operations. Platform IT refers to computer resources, both hardware and software, that are physically part of, dedicated to, or essential in real time to the mission performance of special purpose systems such as weapons, training simulators, diagnostic test and maintenance equipment, calibration equipment, equipment used in the research and development of weapons systems, medical technologies, transport vehicles, buildings, and utility distribution systems such as water and electric. Examples of platform IT interconnections that impose security considerations include: communications interfaces for data exchanges with enclaves for mission planning or execution,

remote administration, and remote upgrade or reconfiguration (DoDD 8500.1, “Information Assurance (IA)” (reference a.).

Privileges – A set of authorization/permissions granted by an authorized officer to an AIS and network or network user to perform certain operations.

Protected Health Information (PHI) – Individually identifiable health information that is a subset of health information, including demographics, that identifies an individual or there is a reasonable basis to believe that the information may be used to identify an individual. This information is created or received by a healthcare provider, health plan, or employer and relates to past, present, or future physical or mental health of an individual; the provision of care or payment for care of that individual. PHI is information that is transmitted or maintained by electronic or any other form or medium.

Public Key Infrastructure – An enterprise-wide service that supports digital signatures and other public key-based security mechanisms for DoD functional domain programs, including generation, production, distribution, control and accounting of public key certificates.

Risk – The probability that a particular threat will exploit a particular vulnerability of the system.

Risk Analysis – The process of identifying security risks, determining their magnitude, and identifying areas needing safeguards. Risk analysis is a part of risk management.

Risk Assessment – An assessment of a system based on the sensitivity of information processed, or to be processed, and the clearances of users to determine the security class of the system.

Risk Management – Achieving and maintaining an acceptable IA posture (i.e., adequate security, interoperability, and visibility within IA situational awareness or command and control systems) through the implementation of assigned IA controls. IA controls are assigned based on the value of the information being processed and the extent of the information environment being shared.

Safeguards – An implementation of technology or techniques to protect confidentiality, integrity, and availability.

Security Evaluation – An evaluation done to assess the degree of trust that can be placed in systems for the secure handling of sensitive information. One type, a product evaluation, is an evaluation performed on the hardware and software features and assurances of a computer product from a perspective that excludes the application environment. The other type, a system evaluation, is done to assess a system’s security safeguards with respect to a specific operational mission and is a major step in the C&A process.

Security Policy – The set of laws, rules, and practices that regulate how an organization manages, protects, and distributes sensitive information.

Security Requirements – The types and levels of protection necessary for equipment, data, information, applications, personnel, and facilities to meet security policy.

Security Safeguards – The protective measures and controls prescribed to meet the security requirements specified for a system. Those safeguards may include but are not necessarily limited to: hardware and software security features, operating procedures, accountability procedures, access and distribution controls, management constraints, personnel security, and physical structures, areas, and devices.

Sensitive Information – Any information, the loss, misuse, modification of, or unauthorized access to, could adversely affect the national interest or the conduct of federal programs, or the privacy to which individuals are entitled under Section 552a of Title 5, U.S. Code, (The Privacy Act) but has not been specifically authorized under criteria established by an Executive Order or an Act of Congress to be kept classified in the interest of national defense or foreign policy.

System Integrity – The quality that a system has when it performs its intended function in an unimpaired manner, free from deliberate or inadvertent unauthorized manipulation of the system.

Threat – Any circumstance or event with the potential to cause harm to a system in the form of destruction, disclosure, modification of data, and/or denial of service.

User – Person or process accessing an IS either by direct connections (e.g., via terminals), or indirect connections (e.g., prepare input data or receive output not reviewed for content or classification by a responsible individual).

User ID – A unique symbol or character strings used by a system to identify a specific user.

Virus – A self-propagating computer program composed of a mission component, a trigger component, and a self-propagating component.

Vulnerability – A weakness in system security procedures, system design, implementation, internal controls, etc. that could be exploited to violate system security policy.

ENCLOSURE 3

ACRONYMS

ADP.....Automated Data Processing
ASD.....Assistant Secretary of Defense
ATOAuthorization to Operate

C&A.....Certification and Accreditation
CIO.....Chief Information Officer

DAADesignated Accrediting Authority
DAARDesignated Accrediting Authority Representative
DIACAP.....DoD Information Assurance Certification and Accreditation Process
DoD.....Department of Defense
DoDDDepartment of Defense Directive
DoDIDepartment of Defense Instruction

HA.....Health Affairs
HDBKHandbook

IAInformation Assurance
IAOInformation Assurance Officer
IAM.....Information Assurance Manager
IATO.....Interim Authorization to Operate
IAVM.....Information Assurance Vulnerability Management
IAWG.....Information Assurance Working Group
IDIdentification
IDSIntrusion Detection System
IS.....Information System
IT.....Information Technology

JMISJoint Medical Information Systems

MHSMilitary Health System

MOAMemorandum of Agreement

MTFMilitary Treatment Facility

OMBOffice of Management and Budget

PEOProgram Executive Officer / Program Executive Office

PHIProtected Health Information

PKIPublic Key Infrastructure

PM.....Program Manager

SASystem Administrator

SI.....Sensitive Information

SSAASystem Security Authorization Agreement

TIWGTechnical Integration Working Group

TMA.....TRICARE Management Activity