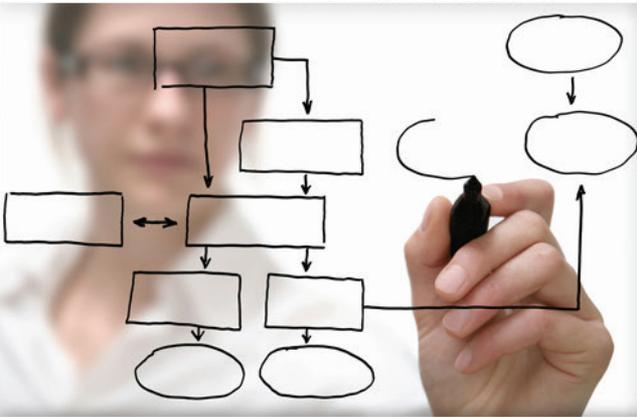


TMA PRIVACY AND CIVIL LIBERTIES OFFICE

2012 HEALTH INFORMATION PRIVACY & SECURITY TRAINING



Military Health System Information Assurance Program

THE POWER OF TEAM WORK
Committed to Protecting Beneficiary Data

Purpose

The purpose of this presentation is to provide an overview of the Military Health System (MHS) Information Assurance (IA) Program and provide insight into the DoD transition to alignment with National Institute of Standards and Technology (NIST) security publications.



MHS IA Program

Objectives

- Upon completion of this presentation, you should be able to:
 - Identify common cyber security threats to information the MHS IA office is concerned with and protects against
 - Describe the functions performed by MHS IA office
 - Identify how MHS IA collaborates with the TMA Privacy and Civil Liberties Office
 - Explain the IA Transformation and DoD's transition to alignment with NIST security publications



MHS IA Program

Protection of Information

Threats



Cyber Espionage



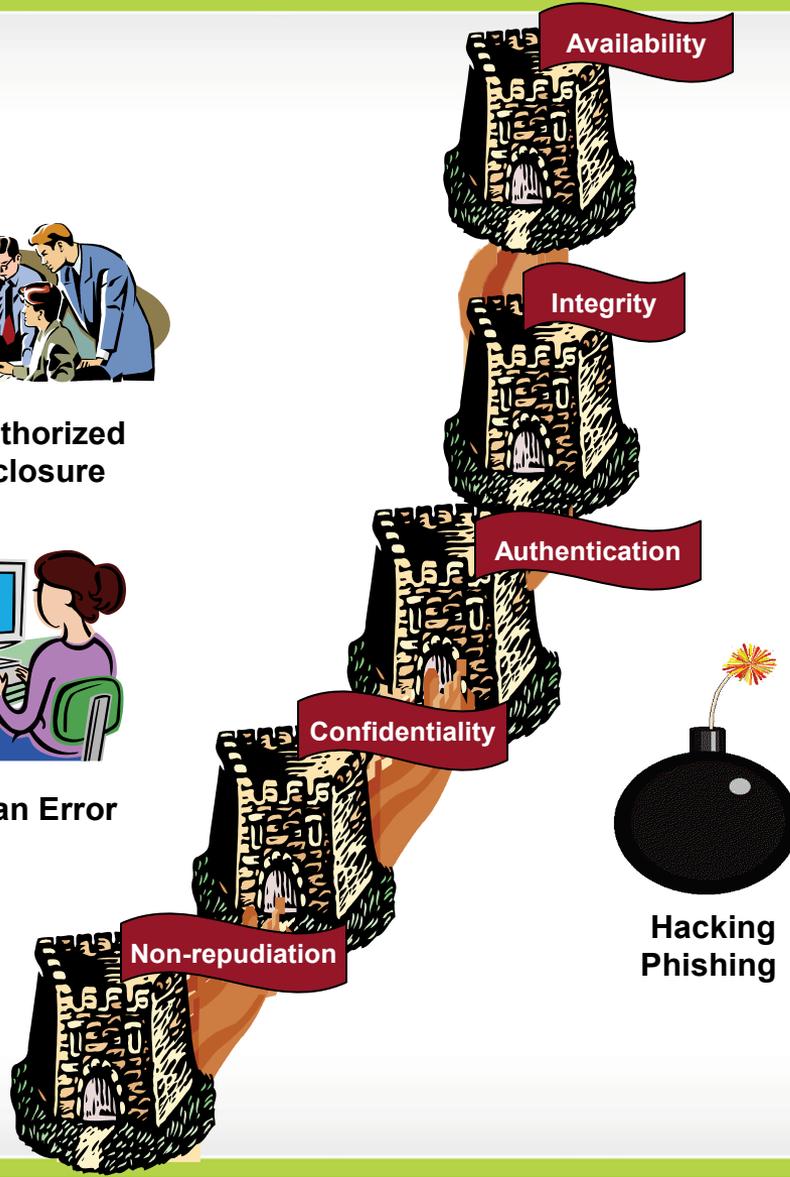
Unauthorized Disclosure



Unsanitized Media



Human Error



Threats



Nation States



Malware



Hacking Phishing



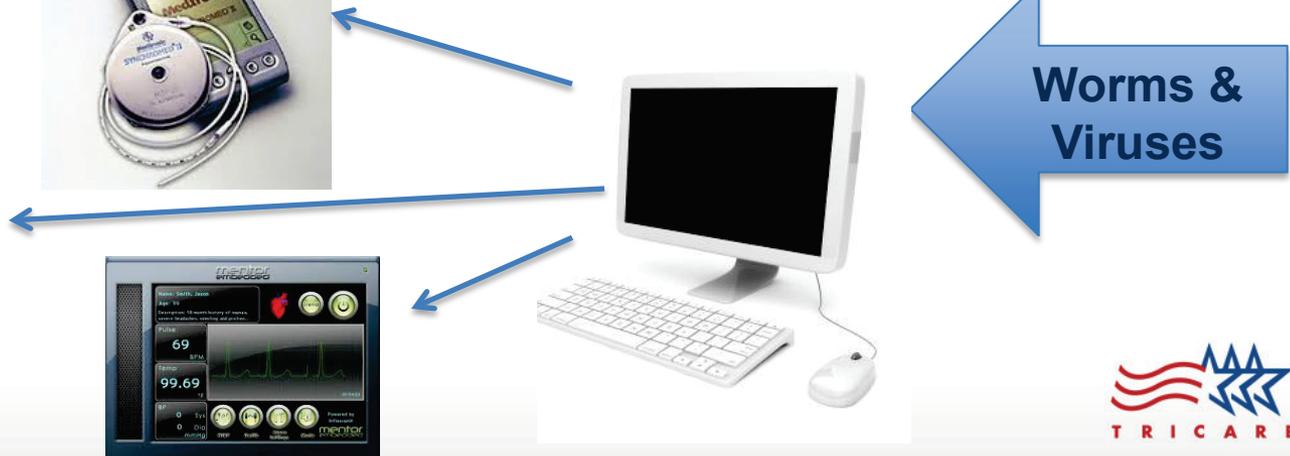
MHS Concerns

- Medical device vulnerabilities
 - The Conficker virus has infected important computerized medical devices (i.e., Pacemakers) through wireless and other local area network connections



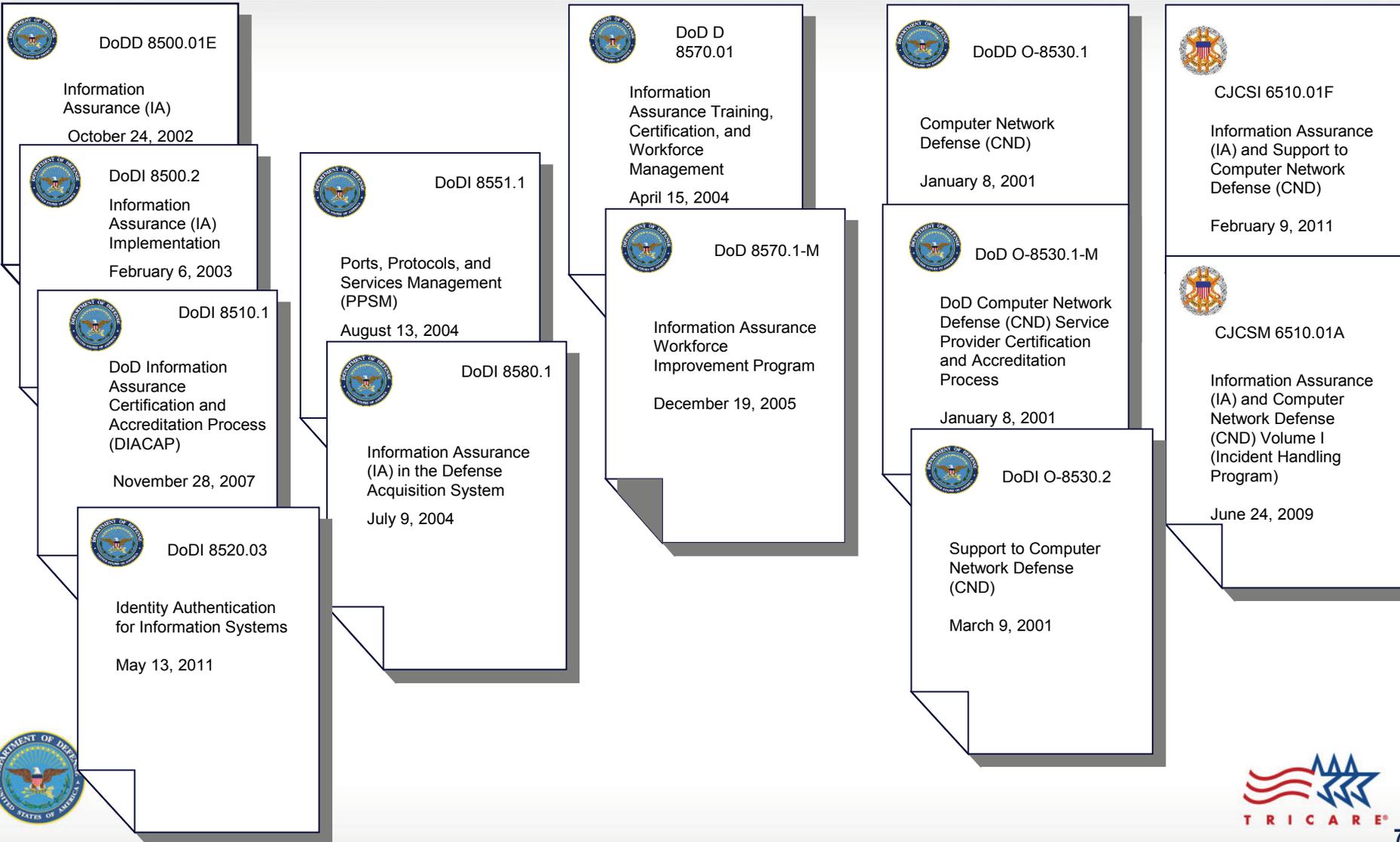
MHS Concerns

- Integrity of electronic medical records
 - Computerized hospital records may be accessed through interconnected systems (hospitals, emergency care facilities, doctors' offices)
 - Portability and transferability of patient records on personal digital assistants and other portable devices without security mechanisms in place, i.e., encryption, passwords, etc.



MHS IA Program

DoD Policy Drives the MHS IA Program



MHS IA Program

MHS IA Policy Guidance Manual

3/5/2004 No.0
Military Health System (MHS) Information Assurance (IA) Policy Guidance Manual

10/10/08 No.1
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Governance

10/10/08 No.2
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Sanitization and Disposal of Electronic Storage Media and MHS Information Technology Equipment Procedures

02/22/12 No.3
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Incident Reporting and Response Program

03/25/09 No.4
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Employee Behavior

02/22/12 No.5
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Physical Security

7/19/05 No.6
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Wireless Local Area Networks (WLANs)

02/22/12 No.7
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Data Integrity

02/02/10 No.8
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Certification and Accreditation (C&A)

10/10/08 No.9
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Configuration Management – Security: Software Usage Marking

10/10/08 No.10
Military Health System (MHS) Information Assurance (IA) Implementation Guide
System Life Cycle Management

10/10/08 No.11
Military Health System (MHS) Information Assurance (IA) Implementation Guide
DoD Public Key Infrastructure (PKI) and Public Key Enabling (PKE)

02/02/12 No.12
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Information Assurance Vulnerability Management (IAVM) Program

05/20/10 No.13
Military Health System (MHS) Information Assurance (IA) Implementation Guide
Information Assurance Education, Training, and Awareness

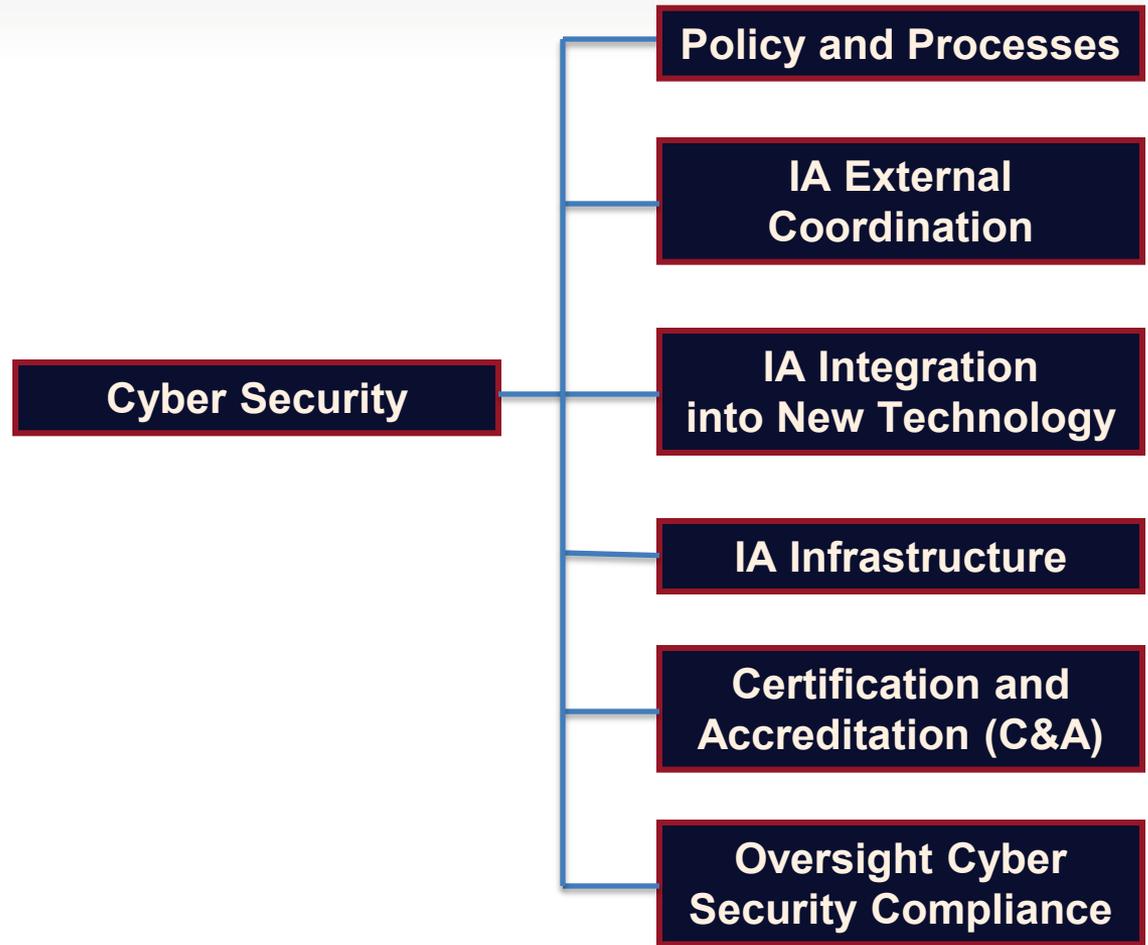
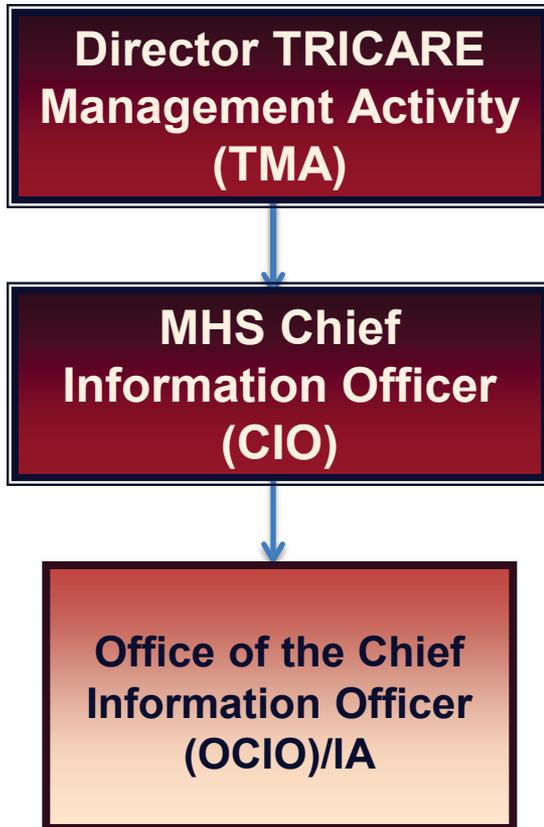
02/10/08 No.14
Military Health System (MHS) Information Assurance (IA) Implementation Guide
INFOCON

TRICARE Management Activity ADMINISTRATIVE INSTRUCTION
NUMBER 041 April 9, 2012
SUBJECT: Risk Assessments for TRICARE Management Activity Information Technology Assets and Applications

TRICARE Management Activity ADMINISTRATIVE INSTRUCTION
NUMBER 025 March 7, 2011
SUBJECT: Conducting Annual Reviews on TMA-Owned or Controlled Information Systems



MHS IA Organization



MHS IA Functions

Policy and Processes

Ensures protection of the enterprise by establishing policies, standards, and processes for the security of information and information systems from internal and external threats and vulnerabilities. Ensures that enterprise-wide developed and maintained information systems do not present a risk to the DoD Information Enterprise. Establishes risk assessment procedures.

IA External Coordination

Coordinates with Department of Veterans Affairs (VA), Department of Health and Human Services (HHS), and commercial entities on the implementation and oversight of information security for health. Maintains liaisons with the DoD CIO Office, Service Component CIO offices, VA, HHS, and external partners to ensure continuous coordination of component IA activities and programs. Coordinates and advocates resources for IA enterprise solutions. Develops and maintains an MHS-wide view of IA requirements that support the protection of DoD health data and systems shared with external partners. Provides oversight of DoD IA education, training, and awareness activities.



MHS IA Functions

IA Integration into New Technology

Defines IA security architecture and processes for new technologies and processes, i.e., distributive development, common services, virtualization, and cloud computing. Ensures that component acquisition processes for emergent technologies incorporate IA planning consistent with the current legislative and DoD Directives. Ensures that IA requirements for emergent technologies are addressed and visible in all investment portfolios and investment programs incorporating DoD information systems. Shares research and technology, techniques, and lessons learned relating to IA with Office of the Secretary of Defense, Service components, and external partners.

IA Infrastructure

Manages the Identity Management and Public Key Infrastructure issuance and registration of server certificates to ensure trusted identities. Manages and coordinates the support requirements for Command Cyber Readiness Inspections and Computer Network Defense Service Provider validations.



MHS IA Functions

C&A

Through an extensive C&A process, ensures that information systems that support the component and that are deployed enterprise-wide conform to the requisite security controls to protect beneficiary information. Implements and manages the C&A process for all enterprise systems. Analyzes and tracks Plan of Actions and Milestones (POA&M), Annual Reviews, and Risk Assessments for Defense Health Information Management System, Defense Health Services Systems, MHS Cyberinfrastructure Services (MCiS), Interagency Program Office (IPO), TMA Directorates, and contractors.

Oversight Cyber Security Compliance

Manages the oversight procedures necessary to ensure compliance with the Information Assurance Vulnerability Management (IAVM) Program, United States Cyber Command issuances, Ports and Protocols management, and Computer Network Defense alerts. Provides enterprise-wide reporting for Federal Information Security Management Act, Congressional Justification Booklet, IA Budget, and DoD Demilitarized Zone White List Registry. Manages TMA response to cyber security incidents. Coordinates with Law Enforcement and Computer Network Defense Service Providers. Manages the incident response team to preserve and collect forensic evidence, restore capabilities, and identify additional protection measures.



TMA Privacy and Civil Liberties Office Support

- Provides support as required
 - Responds to information breaches
 - Incident management
- Confirmation of system compliance with Privacy Impact Assessments in the C&A process



C&A Transformation

- Preparing for transition
 - The DoD is aligning the IA program with the intelligence community and the other executive agencies
 - MHS IA Program is preparing for major changes



MHS IA Program

IA Transformation

Current versions of DoDD 8500.01,
DoDI 8500.2, and DoDI 8510.01

Mission Assurance
Category (MAC) / Confidentiality
Level (CL)

IS Definitions

DoD Defined
Security Controls

C&A Process

*Joint Task Force
Transformation Initiative*

Draft revisions of DoDD 8500.01,
DoDI 8500.02, and DoDI 8510.01

Impact Value: Low / Moderate / High
Security Objectives:
Confidentiality / Integrity / Availability

Expanded IT definition to align with
CNSSI 4009 and encompass new and
emerging capabilities

Using NIST SP 800-53 Security Control Catalogue.
Creating DoD Assignment Values, validation
procedures, and implementation guidance.

Risk Management Framework
includes processes to further mitigate and
remediate risk to systems



IA Transformation

- DoDD 8500.01
 - Remains capstone IA Directive and charters IA Program
- DoDI 8500.02
 - Describes IA Program and shows how issuances fit
 - IA controls to move to knowledge service (KS)
 - Implementation and validation procedures will be on KS
 - DoD will not use NIST SP 800-53A for validation



IA Transformation

- DoD 8500.01 and 8500.02
 - Publication early 4th Quarter CY12
- Committee on National Security Systems Instruction (CNSSI) 1253, “Security Categorization and Control Selection for National Security Systems”
 - Policy for categorization of all DoD information systems
 - Confidentiality/Integrity/Availability and High/Moderate/Low



IA Transformation

- DoDI 8510.01
 - DoD Information Assurance Certification and Accreditation Process (DIACAP) to become Risk Management Framework for DoD information technology
 - Aligns DoD Risk Management Process (formerly C&A) with NIST SP 800-37
 - C&A will become Assessment and Authorization (A&A)
 - Designated Accrediting Authority (DAA) will become Authorizing Official
 - DIACAP KS will be the authoritative source for IA controls, validation procedures, and implementation guidance
 - Re-aligning the current DIACAP package with NIST documents to support inter-departmental reciprocity
 - Publication early 4th quarter CY12



IA Transformation

- From Mission Assurance Categories and Confidentiality Levels to CNSSI 1253 System Categorization Impact Values
 - Low: the loss of confidentiality, integrity, or availability could be expected to have a limited adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States
 - Moderate: the loss of confidentiality, integrity, or availability could be expected to have a serious adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States
 - High: the loss of confidentiality, integrity, or availability could be expected to have a severe or catastrophic adverse effect on organizational operations, organizational assets, individuals, other organizations, or the national security interests of the United States



IA Transformation

- CNSSI 1253 (continued)

- Security categorization

- Security category = {(confidentiality, value), (integrity, value), (availability, value)}
 - Values are low, moderate, or high
- Select initial set of security controls
- Select and apply security control overlays
- DoD developing overlays
 - Privacy/Health Insurance Portability and Accountability Act overlay



New Terminology

OLD	NEW
Senior Information Assurance Officer (SIAO)	Senior Information Security Officer (SISO)
Designated Accrediting Authority (DAA)	Authorizing Official (AO)
Certifying Authority (CA)	Security Control Assessor (SCA)
Information Assurance Manager (IAM)	Information System Security Manager (ISSM)
Information Assurance Officer (IAO)	Information System Security Officer (ISSO)
DIACAP Technical Advisory Group (TAG)	RMF Technical Advisory Group (TAG)
Certification and Accreditation (C&A)	Assessment and Authorization (A&A)



NIST Documents Mapped to DIACAP Package

NIST	DoD
System Security Plan	DIACAP System Identification Profile (SIP)
Security Assessment Report	DIACAP Scorecard
POA&M	POA&M
Continuous Monitoring Plan	NIST SP 800-53 CA-7 Continuous Monitoring
Risk Management Strategy	NIST SP 800-53 PM-9 Risk Management Strategy
Security Assessment Plan	DIACAP SIP and Implementation Plan (DIP)
POA&M Strategy	Knowledge Service Guidance on developing DIACAP POA&M
Authorization Decision Document	DIACAP Scorecard
Security Status Report	Ongoing reporting to AO



Demonstrating Compliance

- DoD will develop standards for implementing and validating the security controls
 - Decompose controls to Control Correlation Identifiers (CCI)
 - Single actionable statements
 - Each CCI will be identified as technical or policy
 - Controls will be linked to Defense Information Systems Agency Security Technical Implementation Guides (STIGs)
 - Identify departmental-level policy that aligns to a control
 - Developing an implementation guidance and validation procedures database
 - Availability will coincide with publication of policy



MHS IA Program

Conclusion

- A successful enterprise-wide cyber security program requires active participation by all members of the community. This is the only way we can ensure that the personal health information of our beneficiaries is protected
- As the DoD transitions to a federally aligned cyber security program, OCIO/IA will implement the policies and procedures to facilitate the transformation



MHS IA Program Summary

- You should now be able to:
 - Identify common cyber security threats to information the MHS IA office is concerned with and protects against
 - Describe the functions performed by MHS IA office
 - Identify how MHS IA collaborates with the TMA Privacy and Civil Liberties Office
 - Explain the IA Transformation and DoD's transition to alignment with NIST security publications

