



HEALTH AFFAIRS

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE

WASHINGTON, DC 20301-1200

OCT 10 2008

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

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

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

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

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

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

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

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



Charles M. Campbell
Chief Information Officer
Military Health System

Attachments:

As stated

cc:

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

 <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS) INFORMATION ASSURANCE (IA) IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 14	
	EFFECTIVE DATE 07/19/05	REVISED DATE 10/10/08
<p>Subject:</p> <p style="text-align: center;">INFORMATION OPERATION CONDITION (INFOCON)</p>		

1. PURPOSE AND SCOPE

1.1. The provisions of this guide are policy for all TRICARE Management Activity (TMA) Components (TRICARE Management Activity (TMA) Directorates; TRICARE Regional Offices (TRO), and the Program Executive Office (PEO), Joint Medical Information Systems Office (JMISO)) (hereafter referred to as the TMA Component(s)). For TRICARE Contractors, this document is policy if required by contract; otherwise it serves as information assurance guidance. The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures.

1.2. This implementation guide provides a framework within which network managers can increase the measurable readiness of TMA enclaves. The Information Operations Condition (INFOCON) system provides authority, discretion, and accountability to prepare the MHS networks and information systems at any level deemed appropriate for the current and anticipated environment. The term “MHS Information System (IS)” encompasses all automated IS applications, enclaves, outsourced IT-based processes, and platform information technology (IT) interconnections as defined in Department of Defense (DoD) Instruction (DoDI) 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003.

1.3. The INFOCON system is executed through the operational authority of Commander, United States Strategic Command (CDRUSSTRATCOM) in accordance with (IAW) DoDD O-8530.1, “Computer Network Defense (CND),” January 8, 2001, as cited in Department of Defense Directive (DoDD) 8500.01E, “Information Assurance (IA),” October 24, 2002, certified current as of April 23, 2007.

2. POLICY

2.1. The Director, TMA retains the authority to set INFOCON levels for TMA information systems and networks. These levels must remain at least as high as the DoD INFOCON level declared by CDRUSSTRATCOM.

2.2. INFOCON strategy is a “readiness-based,” proactive approach to Computer Network Defense (CND).

2.3. INFOCONs are a uniform system of five progressive readiness conditions - INFOCON 5, INFOCON 4, INFOCON 3, INFOCON 2, and INFOCON 1. Each level represents an increasing level of network readiness based on tradeoffs in resource balancing.

2.4. The Commander, Joint Task Force for Global Network Operations (CJTF-GNO) will recommend changes in DoD INFOCON to CDRUSSTRATCOM. Prior to this recommendation, CJTF-GNO will coordinate with the DoD Components to determine the operational impact of changing the DoD INFOCON level.

2.5. INFOCON measures should not result in a self-imposed denial of service, either to specific users or to entire networks. When necessary, measures will be carefully and narrowly tailored to focus on the specific situation.

2.6. The Defense Information Systems Agency (DISA) is the Computer Network Defense Service Provider (CNDSP) for TMA.

2.7. INFOCON measures should mitigate insider threats from both authorized and unauthorized users.

2.8. INFOCON levels are:

2.8.1. INFOCON 5 (normal activity). This is the normal state of readiness of information systems and networks (i.e., “Routine” Network Operations (NetOps)) that can be sustained indefinitely. System and network administrators will create and maintain a snapshot of each server and workstation in a normal operational condition. This snapshot then becomes the normal operational baseline that can be compared against future changes to identify unauthorized activities.

2.8.2. INFOCON 4 (increased vigilance procedures). System and network administrators will establish an operational rhythm to validate the known good image of an information network against the current state and identify unauthorized changes. Additionally, user profiles and accounts are reviewed and checks are conducted for dormant accounts. Impact to MHS end-users should be negligible.

2.8.3. INFOCON 3 (enhanced readiness procedures). System and network administrators will further NetOps readiness by increasing the frequency of validation of the information network and its corresponding configuration. Impact to MHS end-users should be minor.

2.8.4. INFOCON 2 (greater readiness procedures). System and network administrators will increase the frequency of validation of NetOps readiness for the information network. Impact to MHS end-users could be significant for short periods, which can be mitigated through training and scheduling.

2.8.5. INFOCON 1 (maximum readiness procedures). This is the highest condition of NetOps readiness. This condition addresses intrusion techniques that cannot be identified or

defeated at lower readiness levels. INFOCON 1 is the most effective method for ensuring the system has not been compromised. During INFOCON 1, System and Network Administrators may reload the operating system software on key infrastructure servers from an accurate baseline. Once baseline comparisons no longer indicate anomalous activities, INFOCON 1 would be terminated. Impact to MHS end-users could be significant for short periods, which can be mitigated through training and scheduling.

2.9. Tailored Readiness Options (TROs). TROs are supplemental measures to respond to specific intrusion characteristics. They are narrowly focused and meant to supplement the current INFOCON readiness level. TROs will document, in standard language, all supplemental INFOCON measures to ensure a common understanding of the level of readiness and mission impact of each measure.

3. PROCEDURES

3.1. CDRUSSTRATCOM will notify the Director, TMA of a DoD-level INFOCON change via a Computer Network Event Conference (CNEC) and/or a DoD INFOCON Alert message.

3.2. The Director, TMA will acknowledge establishment of the appropriate INFOCON operational rhythm via an acknowledgement message within 24 hours of receipt of the INFOCON Alert Message.

3.3. The Director, MHS Office of the Chief Information Officer/Information Assurance (OCIO/IA) will acknowledge receipt of the INFOCON alert.

3.4. The Director, TMA retains the authority to declare INFOCON changes for TMA information systems and networks.

3.5. The INFOCON level declared by Director, TMA must remain at least as high as the DoD INFOCON level or the level prescribed by a higher authority in their chain of command.

3.6. The Director, TMA will notify CDRUSSTRATCOM and JTF-GNO and the services if the INFOCON level is independently raised in order to provide situational awareness and allow them to consider matching the regional level to better support operations.

3.7. TMA Network Managers are responsible for implementing INFOCON requirements.

3.8. TMA Network Managers will compose the INFOCON Status Situation Report (SITREP) whenever the INFOCON status changes (See Strategic Command Directive (SD) 527-1 dated 27 Jan 2006, Reference 4).

3.9. TMA Network Managers will compose the Local INFOCON Change SITREP to report TMA changes in INFOCON level, and to report INFOCON changes declared by TMA.

3.10. The Director, OCIO/IA will consolidate SITREPS and report to USSTRATCOM and JTF-GNO.

3.11. Returning the system to a pristine, baseline state restores confidence in the system. Any system changes, while not always easily detectable in isolation, are almost always detectable by comparing the current status to a previous known baseline.

4. REFERENCES

1. DoDD 8500.01E, “Information Assurance (IA),” October 24, 2002, certified current as of April 23, 2007
2. DoDI 8500.2, “Information Assurance (IA) Implementation,” February 6, 2003
3. DoDD O-8530.1, “Computer Network Defense”, January 8, 2001
4. Strategic Command Directive (SD) 527-1, “Operations, Planning, and Command and Control: Department of Defense (DoD) Information Operations Condition (INFOCON) System Procedures,” January 27, 2006 (U/FOUO)

5. ACRONYMS

CDRUSSTRATCOM	Commander, United States Strategic Command
CJCSI	Chairman of the Joint Chiefs of Staff Instruction
CJTF-GNO	Commander, Joint Task Force for Global Network Operations
CIO	Chief Information Officer
CND	Computer Network Defense
CNDSP	Computer Network Defense Service Provider
CNEC	Computer Network Event Conference
DISA	Defense Information Systems Agency
DoD	Department of Defense
DoDD	Department of Defense Directive
DoDI	Department of Defense Instruction
HA	Health Affairs
IA	Information Assurance
IAW	In Accordance With
INFOCON	Information Operations Condition
IS	Information System
IT	Information Technology
JMIS	Joint Medical Information Systems
MHS	Military Health System
NetOps	Network Operations
PEO	Program Executive Office
SITREP	Situation Report
TMA	TRICARE Management Activity
TRO	TRICARE Regional Offices
TRO	Tailored Readiness Option