

 <p style="text-align: center;">MILITARY HEALTH SYSTEM (MHS)</p> <p style="text-align: center;">INFORMATION ASSURANCE (IA)</p> <p style="text-align: center;">IMPLEMENTATION GUIDE</p>	IMPLEMENTATION GUIDE No. 12	
	EFFECTIVE DATE 07/19/05	REVISED DATE 02/22/12
<p>Subject:</p> <p style="text-align: center;">INFORMATION ASSURANCE VULNERABILITY</p> <p style="text-align: center;">MANAGEMENT (IAVM) PROGRAM</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),) (hereafter referred to as the TMA Component(s)). The Chief Information Officers of the Service Medical Departments are encouraged to incorporate this document into their information assurance policies and procedures.

1.2. The Information Assurance Vulnerability Management (IAVM) process provides positive control of vulnerability notification and corresponding corrective action for TMA system/ network assets. Vulnerabilities in computing systems and networks are weaknesses that could compromise sensitive or patient health information and deny service to beneficiaries of TMA.

1.3. This implementation guide establishes responsibilities and procedures for the TMA IAVM program, to include organizational and individual responsibilities, registration, compliance criteria, Plan of Action and Milestones (POA&M), enforcement, and verification, in accordance with (IAW) Chairman, Joint Chief of Staff Instruction (CJCSI) 6510.01F, "Information Assurance and Support to Computer Network Defense (CND)," 9 February 2011. This implementation guide establishes responsibilities and procedures IAW Chairman, Joint Chief of Staff Manual (CJCSM) 6510.01A 24 June 2009.

2. POLICY

2.1. It is TMA policy that TMA Components shall monitor and report mitigation of known Information Assurance Vulnerability Alerts (IAVAs) to the TMA IAVM Coordinator through the Department of Defense (DoD) Vulnerability Management System (VMS).

3. PROCEDURES

3.1. The Designated Accrediting Authority (DAA) shall:

- 3.1.1. Ensure IAVM notices are available to all Information Assurance Managers (IAMs), Information Assurance Officers (IAOs), and System Administrators (SAs) as required.
- 3.1.2. Review POA&Ms and, if appropriate, disconnect compromised systems from the network immediately if unable to comply with the IAVM notice.
- 3.1.3. Monitor IAVM compliance and overall status for those assets under their control and ensure compliance is reported as required.
- 3.1.4. Review and approve submitted plans for patch testing for systems requiring assured availability.

3.2. The Certifying Authority (CA) shall:

- 3.2.1. Review POA&Ms and, if appropriate, recommend disconnecting compromised systems from the network immediately if unable to comply with the IAVM notice.

3.3. The Certifying Authority Representative shall:

- 3.3.1. Review and analyze POA&Ms mitigations and submit recommendations to CA.
- 3.3.2. If appropriate, recommend disconnecting compromised systems from the network immediately if unable to comply with the IAVM notice.

3.4. The TMA IAVM Coordinator shall:

- 3.4.1. Serve as primary point of contact (POC) for US Cyber Command (USCC).
- 3.4.2. Acknowledge receipt of IAVA and IAVB notices within VMS by the specified acknowledgement date.
- 3.4.3. Revises VMS organizational structure as necessary.
- 3.4.4. Disseminate IAVM notices to the appropriate TMA Component Program of Record (POR) Program Manager and asset owners.
- 3.4.5. Generate a compliance report for TMA Components using VMS and send to CA.
- 3.4.6. Generate monthly TMA compliance reports for the TMA Chief Information Officer (CIO).
- 3.4.7. Provide TMA compliance reports to the TMA OCIO/IA staff.

- 3.4.8. Monitor TMA Components' compliance.
 - 3.4.9. Develop and present the IAVM Status Report briefing at quarterly Information Assurance Working Group (IAWG) meetings.
 - 3.4.10. Respond to requests for VMS user account creation, technical support, password resets, etc.
 - 3.4.11. Respond to requests for VMS user account creation and termination, technical support, password resets, and miscellaneous requests.
- 3.5. Program of Record (POR) Program Managers (PM) of Centrally Managed Programs shall:
- 3.5.1. Register with the VMS for a User Identification (ID) and password for VMS.
 - 3.5.2. Designate a primary and secondary IAVM point of contact (POC).
 - 3.5.3. Respond to each IAVM message as the system configuration manager.
 - 3.5.4. Monitors & Notifies Program Offices of newly issued IAVM Notices and the date they are required to be in compliance.
 - 3.5.5. Provide periodic status updates, as required, throughout the life cycle of the vulnerability until the corrective action has been completed.
 - 3.5.6. Ensure dissemination of the program action plan, if necessary, to affected SAs.
 - 3.5.7. Process program level POA&Ms through the DAA.
 - 3.5.8. Create and maintain a hierarchical organizational structure for their assets within VMS.
- 3.6. The IAM and IAO shall:
- 3.6.1. Ensure IAVM notices are disseminated to the lowest level IAOs, SAs, and other individuals identified as participants in the IAVM process.
 - 3.6.2. Ensure system names in VMS match the DoD Information Technology Portfolio Repository (DITPR) system names.
 - 3.6.3. Ensure all subordinate organizations comply with all IAVMs within the designated compliance window.
 - 3.6.3.1. If compliance with the designated timeframe is not possible, a POA&M must be developed.

- 3.6.4. Monitor IAVB notices.
 - 3.6.5. Review and develop POA&Ms; monitor POA&Ms with their associated mitigation plans and implementation timelines as required.
 - 3.6.6. Ensure that all required risk mitigation actions are implemented in accordance with associated timeline, once POA&M is approved.
 - 3.6.7. Ensure compliance checks of their subordinate organizations are conducted to ensure mitigation and/or corrective actions are completed.
 - 3.6.8. Maintain positive configuration control of all Information Systems (ISs) and/or assets under their purview. Maintain configuration documentation that identifies specific system and/or asset owners and SAs, including applicable network addresses.
 - 3.6.9. Ensure networked assets are managed and administered in a manner allowing both chain of command and authorized independent verification of corrective actions.
 - 3.6.10. Ensure scanning data is uploaded to VMS to present a near-real time view of vulnerability management across the Global Information Grid (GIG).
 - 3.6.11. Create and maintain a hierarchical organizational structure for their assets within VMS.
 - 3.6.12. Monitor scanning and remediation activity, as required, in response to each released IAVM notice and for all other applicable vulnerabilities.
 - 3.6.13. Ensure devices are scanned for vulnerabilities, at least monthly and monitor patching process.
- 3.7. The Program Office IAVM representatives shall:
- 3.7.1. Register with the TMA IAVM Coordinator for assignment of user ID and password in the VMS system.
 - 3.7.2. Disseminate IAVM notices to lowest level SAs.
 - 3.7.3. Enter their organization's acknowledgment and compliance and/or POA&M data into VMS.
 - 3.7.4. Monitor compliance status of IAVM notices, and update VMS as statistics change throughout the life cycle of the IAVM notice.
 - 3.7.5. Review and submit plans for patch testing to the POR PMs or IAO/IAM

as appropriate for approval for systems requiring assured availability, if appropriate.

- 3.7.6. Ensure scanning data is uploaded to VMS to present a near-real time view of vulnerability management across the GIG.
- 3.7.7. Create and maintain a hierarchical organizational structure for their assets within VMS.
- 3.7.8. Monitor scanning and remediation activity, as required, in response to each released IAVM notice and for all other applicable vulnerabilities, IAW CJCSM 6510.01E.
- 3.7.9. Ensure scanning for all devices for vulnerabilities at least monthly and monitor patching, if necessary.
- 3.7.10. Ensure scanning for all networked devices for vulnerabilities at least monthly and monitor patching, if necessary.

3.8. The SA shall:

- 3.8.1. Ensure all devices are IAVM compliant prior to connecting the devices to DoD networks.
- 3.8.2. Respond to all active IAVMs; any asset found with an active vulnerability, where the IAVM completion date has closed, must be brought into compliance immediately, must have a POA&M submitted and approved or the asset must be disconnected.
- 3.8.3. Create plans for patch testing and forward to the designated IAVM representatives for approval for systems requiring assured availability.
- 3.8.4. Test and evaluate all patches intended to resolve an IAVM notice unless the Program Of Record process applies. Monitor appropriate web sites for new vulnerability notices.
- 3.8.5. Report compliance and/or POA&M information through the command channels for aggregation and reporting.
- 3.8.6. If unable to comply with the notice, prepare and submit a POA&M (including implementation timelines) prior to the time specified in the IAVM notice (usually 21days). Submitted POA&Ms must be reviewed and approved by the DAA prior to the IAVM notice mitigation date.
- 3.8.7. Perform scanning with Secure Configuration Compliance Validation Initiative (SCCVI) for all devices for vulnerabilities, at least monthly and populate the

scanning in the Secure Configuration Remediation Initiative (SCRI). Use the SCCVI scan data to prioritize remediation efforts and to ensure that all assets are also reported by the SCRI tool or manually.

- 3.8.8. Following each remediation action, SCRI should automatically upload asset data to VMS (or manually by the SA) in order to present a near-real time view of vulnerability management across the GIG.

3.9. IAVA POA&M Process and Timelines

- 3.9.1. Program Offices may operate non-compliant assets only with an approved POA&M.
- 3.9.2. Non-compliant assets must list the vulnerability in the system POA&M.
 - 3.9.2.1. If a system already has a POA&M due to other vulnerabilities, update that POA&M to include any new vulnerabilities.
 - 3.9.2.2. If a system does not have a POA&M, then a new POA&M must be created and submitted.
- 3.9.3. Program Offices must maintain an approved POA&M with implemented mitigation actions until assets are brought into compliance or assets are removed from the network.
- 3.9.4. Program Office provides the IAVM Coordinator with POAM hardcopy and submits the write-up in VMS for review.
- 3.9.5. IAVM Coordinator recommends POAM approval to the CA.
- 3.9.6. CA recommends the POAM approval to the DAA.
- 3.9.7. DAA approves POA&Ms. Approval must be based on a sound POA&M with mitigation actions that minimize the risk of compromise to local systems. Local DAAs must consider the associated risk shared by other DoD networks when approving a POA&M.
- 3.9.8. Failure to have a DAA approved POA&M will result in TMA being placed on the JTF-GNO Watch List.

3.10 VMS User Enrollment and Training.

- 3.10.1. All users assigned responsibility to update or monitor IAVM compliance in VMS shall apply for and obtain a VMS account.
- 3.10.2. The TMA IAVM Coordinator shall create VMS accounts and assign

appropriate permissions, or afford heads of Program Offices to assign permissions to their subordinate users.

3.10.3 Individuals applying for a VMS account shall complete and submit a DD Form 2875, "System Authorization Access Request (SAAR)," August 2009 to the system owner and PO IAO for approval. IAO should forward signed forms to the TMAVMS Coordinator for account creation.

3.10.4. Applicants should meet the minimum qualifications prior to applying for VMS account.

3.10.5. For United States (U.S.) citizens: Possess a National Agency Check (NAC) or higher investigation for Non-secure Internet Protocol Router Network (NIPRNet), and a minimum of a secret clearance for Secret Internet Protocol Router Network (SIPRNet) access.

3.10.6. For non-U.S. citizens: DoD policies state that the required investigation must be completed and favorably adjudicated prior to authorizing Automatic Data Processing/Information Technology (ADP/IT) access to DoD systems/networks. Interim approvals are not authorized to non U. S. citizen contractor employees for access to DoD systems/networks.

3.10.7. Training is available through DISA and within the VMS application. New VMS users should review the computer based training available within the VMS application, or contact the TMA IAVM Coordinator for live DISA training. The TMA IAVM Coordinator can direct the user to the VMS training link, where class times and dates are located.

3.11. Non-Compliance Notification and Enforcement Procedures

3.11.1. USCC shall notify the TMA IAVM Coordinator to provide a status report for non-compliant assets and to coordinate a resolution. This is done via the SIPRNET, typically the day after IAVAs are due. The USCC POC will email the TMA IAVM POCs to alert them of their findings, and it is the TMA IAVM POCs mission to resolve any non-compliant assets.

3.11.2. TMA shall be considered non-compliant under any of the following conditions:

3.11.3. Failure to report IAVM compliance.

3.11.4. Incidents resulting from exploitation of IAVM vulnerability.

3.11.5. Non-compliant assets identified by outside scans, audits, or inspections.

3.11.6. Missing or incomplete Plan of Action and Milestones (POA&M).

3.11.7. A pattern of organization IAVM non-compliance and/or failure to identify causes and take corrective action.

3.11.8. If TMA is not responsive or fails to follow through with resolving the noncompliance, USCC will release an IAVA non-compliance message addressed to the Director, TMA.

3.11.9. TMA must respond within four (4) working days that assets have been brought into compliance or report reasons for non-compliance, planned corrective actions, mitigation plan, and operational impact.

3.11.10. USCC will review TMA corrective actions and coordinate any additional actions required to mitigate any vulnerability created by non-compliance in accordance with Paragraph 5.12.5, DoD Directive O-8530.1, "Computer Network Defense," 8 January 2001.

3.11.11. USCC Shall determine global operational impact of continued IAVA non-compliance as required.

If USCC or TMA has an issue that cannot be resolved concerning compliance actions ASD (NII) and the Chairman, Joint Chiefs of Staff shall be informed.

4. REFERENCES

1. CJCSI 6510.01F, "Information Assurance and Support to Computer Network Defense (CND)," 9 February 2009
2. CJCSM 6510.01B Information Assurance (IA) and Computer Network Defense (CND) Volume I (Incident Handling Program) 22 August 1997
3. DoDI O-8530.1, "Computer Network Defense (CND)," 8 January 2001

5. ACRONYMS

ADP	Automated Data Processing
CC/S/A	Combatant Commands, Services, and Agencies
CIO	Chief Information Officer
CND	Computer Network Defense
DAA	Designated Accrediting Authority
DISA	Defense Information Systems Agency
GIG	Global Information Grid
IA	Information Assurance
IAM	Information Assurance Manager
IAO	Information Assurance Officer
IAVA	Information Assurance Vulnerability Alert
IAVB	Information Assurance Vulnerability Bulletin
IAVM	Information Assurance Vulnerability Management
IAWG	Information Assurance Working Group
IS	Information System
IT	Information Technology
MHS	Military Health System
NAC	National Agency Check
NIPRNet	Non-secure Internet Protocol Router Network
PEO	Program Executive Office
PM	Program Manager
POA&M	Plan of Action and Milestones
POC	Point of Contact
POR	Program of Record
SA	System Administrator
SAAR	System Access Authorization Request
SCCVI	Secure Configuration Compliance Validation Initiative
SCRI	Secure Configuration Remediation Initiative

SIPRNet	Secret Internet Protocol Router Network
TMA	TRICARE Management Activity
TRO	TRICARE Regional Offices
USCC	United States Cyber Command
VMS	Vulnerability Management System