



TRICARE
MANAGEMENT
ACTIVITY

OFFICE OF THE ASSISTANT SECRETARY OF DEFENSE
HEALTH AFFAIRS
SKYLINE FIVE, SUITE 810, 5111 LEESBURG PIKE
FALLS CHURCH, VIRGINIA 22041-3206

AUG - 3 2007

MEMORANDUM FOR: DEPUTY SURGEON GENERAL OF THE ARMY
DEPUTY SURGEON GENERAL OF THE NAVY
DEPUTY SURGEON GENERAL OF THE AIR FORCE
PROGRAM EXECUTIVE OFFICER, JOINT MEDICAL
INFORMATION SYSTEMS
CHIEF ENTERPRISE ARCHITECT, MILITARY HEALTH
SYSTEM
DIRECTOR, NETWORK OPERATIONS DIVISION,
INFORMATION MANAGEMENT, TECHNOLOGY &
REENGINEERING

SUBJECT: Military Health System Operating Systems Guidance

- References:
- (a) DoD Directive 8500.01E, "Information Assurance (IA)," October 24, 2002
 - (b) DoD Memorandum "Internet Protocol Version 6 (IPv6) Policy Update" dated August 16, 2005
 - (c) Department of Defense (DoD) Information Technology Standards Registry (DISR)," at <https://disronline.disa.mil/a/DISR/index.jsp>
 - (d) OMB Memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems" dated March 22, 2007

This memorandum supersedes "Military Health System Operating Systems Guidance," July 21, 2006, and updates guidance for selection of operating systems within the MHS for all acquisitions using Defense Health Program funds. By limiting the diversity of operating systems, the MHS achieves economies of scale, increased interoperability, and reduced complexity in network configurations. This policy/guidance is policy for all MHS centrally-managed Information Systems and networks under the authority of the MHS CIO, and it is guidance for Service specific applications. This guidance was developed, coordinated, and approved by the MHS Technical Integration Working Group and also approved by the MHS Enterprise Architecture Board.

The choice of operating system (OS) is contingent on many and varied factors, however, all operating systems should be compliant with references (a), (b), (c), and the

POSIX standard. In this spirit, the guidance/policy recognizes multiple categories which include: desktop, servers, application/Web servers, virtual machines, etc.

New acquisitions or upgrades of operating systems for the desktop environment should use commercially available Microsoft Windows products. To maintain interoperability, MHS Program Managers should be cognizant of the current versions of desktop operating systems prior to deployment. For MHS Centrally Managed Programs and the TMA Network, the MHS requires the following:

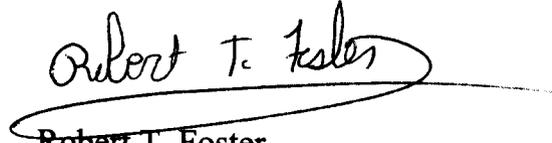
1. All desktops must be in compliance with the security configuration requirements of reference (d) or subsequent updates.
2. In preparation for a migration to Microsoft Vista, all Centrally Managed and TMA Network end user devices should be tested for compatibility and results reported to the MHS CIO.

Service Medical Departments should allow time for Centrally Managed Programs to plan, modify, test, and implement software versions compatible with the new operating system. Applications requiring a desktop operating system other than the Microsoft family are not authorized.

Server operating systems must provide for a secure operating environment satisfying the functional requirement. Continued use of the Microsoft Windows family of server operating systems is recommended for common use servers providing services in an Office Automation environment (such as file and print servers). Programs should initialize plans for a migration from Microsoft Windows Server 2003 OS to the next release of Windows Server. Mainstream support by Microsoft for Windows 2003 Server ends June 2008 and security update support ends June 2013.

The Microsoft Windows family of server operating systems will suffice for most computing requirements. Centrally Managed Programs should continue to analyze the operating system that best meets the individual program's functional requirement. In cases where a Centrally Managed Program's application/Web server is resident on a service-controlled network, a waiver must be submitted and adjudicated in a timely manner before a non-Windows OS can be used, according to the process defined in the Attachment. This guidance is intended for new and existing systems where the selection of an Operating System will not cause an extensive redesign.

This guidance will be updated either annually or as required to reflect advances in technology, product availability, and market support. The point of contact for this guidance is the Technology Management, Integration and Standards Directorate, which can be reached at (703) 681-8701 or by electronic mail at tmisweb@tma.osd.mil.

A handwritten signature in black ink that reads "Robert T. Foster". The signature is written in a cursive style and is underlined with a single horizontal line.

Robert T. Foster
Acting, Chief Information Officer
Military Health System

Attachment:
As stated

Military Health System Operating Systems Guidance
Waiver process for Centrally Managed Programs

- The program office must provide a business case which documents either that no product in the Windows family will technically support the requirement or that the alternate operating system provides an economic benefit over its life cycle.
- The Technical Integration Working Group (TIWG) representative from the Joint Medical Information Systems Office (JMISO) shall present the waiver request with the required justification to the TIWG before the Milestone A decision.
- TIWG voting members will brief their respective managers and be prepared to vote.
- The TIWG will provide a technical recommendation to the Enterprise Architecture Board (EAB).
- The EAB will adjudicate the waiver.
- The EAB will send a recommendation to the MHS CIO. The MHS CIO provides approval/disapproval of waiver requests.