



HEALTH AFFAIRS

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

DEC 05 2005

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

SUBJECT: Military Health System Operating Systems Guidance

- Reference:
- (a) DoD Directive 8500.1, "Information Assurance (IA)," October 24, 2002
 - (b) DoD CIO Memorandum, subject: "Internet Protocol Version 6 (IPv6) Interim Transition Guidance," September 29, 2003
 - (c) Department of Defense (DoD) Information Technology Standards and Profile Registry (DISR)," at <http://disronline.disa.mil>

This memorandum supersedes Military Health System (MHS) Operating Systems Guidance of July 2, 2004, and establishes Office of the Assistant Secretary of Defense (Health Affairs) guidance for selection of operating systems within the MHS. This guidance was developed, coordinated and approved by the MHS Technical Integration Working Group. By limiting the diversity of operating systems, the MHS achieves economies of scale, increased interoperability, and reduced complexity in network configurations. Moreover, decreasing diversity in operating systems within the MHS furthers business process reengineering by simplifying the integration of common functions and by allowing a single, integrated information management approach. This policy/guidance is policy for all MHS centrally managed Information Systems (ISs) and networks under the authority of the MHS CIO and guidance for Service specific applications.

The choice of operating system is contingent on many and varied factors, such as the anticipated load on the device, the type of hardware required to support that load on the device, the type of hardware required to support that load, vendor support for different operating systems and hardware platforms, availability of support personnel, the overall

cost of different solution models, and the regulatory environment within which the device must operate. Furthermore, all operating systems should be compliant with references (a), (b), (c) and the POSIX standard. In this spirit, the guidance/policy is divided into three categories: desktop, common use servers, and application/Web servers.

New acquisitions or upgrades of operating systems for the desktop environment should use a commercially available version of a Microsoft Windows operating system. In an effort to maintain interoperability within the MHS, all centrally managed applications should be cognizant of the current versions of desktop operating systems prior to deployment. Service Medical Departments should notify my office of any planned migration to a newer version of the Microsoft family of operating systems. Service Medical Departments should allow six months for centrally managed MHS 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. MHS centrally managed applications will continue to support Windows 2000 Professional until June 30, 2005, and are no longer required to support their applications in environments controlled by Windows NT, 95, 98, 98SE or ME. Centrally managed applications should note that mainstream support by Microsoft for Windows 2000 Professional ends June 2005 and security update support will end June 2010.

Server operating systems must provide for a secure operating environment and match 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).

It is anticipated that the Microsoft Windows family of server operating systems will suffice for most of the MHS computing requirements. Centrally Managed Programs should consider a migration from Windows 2000 Server OS to Microsoft Windows Server 2003 OS in the future because mainstream support by Microsoft for Windows 2000 Server ends June 2005 and security update support ends June 2010. 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, according to the process defined in Attachment 1, before a non-Windows OS can be used. This guidance is intended for new or existing systems where the selection of an Operating System will not cause an extensive redesign.

Should you require additional information, please contact the Office of Technology Management, Integration and Standards at (703) 681-6779 or tmisweb@tma.osd.mil.

A handwritten signature in black ink, appearing to read 'C. Hendricks', written in a cursive style.

Carl E. Hendricks
Chief Information Officer
Military Health System

Attachment:
Waiver Process for Centrally Managed Programs

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 the life cycle of the product/system.
- The Technical Integration Working Group (TIWG) representative from the Joint Medical Information Systems (JMIS) office 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 for their organization.
- The TIWG will provide a technical recommendation for coordination by the Enterprise Architecture Board (EAB).
- The EAB will adjudicate the waiver and decide on the course of action.
- The EAB will send a recommendation to the MHS CIO. The MHS CIO provides final approval or denial of all waiver requests.