DEPARTMENT OF HEALTH & HUMAN SERVICES
Centers for Medicare & Medicaid Services
7500 Security Boulevard, Mail Stop N3-15-25
Baltimore, Maryland 21244-1850

CMS
CENTERS for MEDICARE & MEDICAID SERVICES

OFFICE OF INFORMATION SERVICES

MEMORANDUM

DATE: **May 3, 2012**

TO: CMS

FROM: Teresa Fryer

Chief Information Security Officer (CISO) and
Director, Enterprise Information Security Group (EISG)

SUBJECT: Minimum Security Configuration Standards

Based on the attached memo dated May 2, 2012 entitled HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications, the *Centers for Medicare and Medicaid Services* (*CMS) Minimum Security Configuration Standards for Operating Systems*, dated February 4, 2010 is rescinded.

When selecting software or operating system configuration standards, CMS' Configuration Management Control (CM-6) from the CMS Acceptable Risk Safeguards (ARS) is still applicable when implementing the proper configuration settings. Please refer to the attached memo when establishing the required security configuration baselines for the intended IT product.

If you have any questions concerning this matter, the Enterprise Information Security Group is available to support staff level questions at CISO@cms.hhs.gov.

teresa.fryer@cms.hhs.gov

Digitally signed by teresa.fryer@cms.hhs.gov
DN: cn=teresa.fryer@cms.hhs.gov
Date: 2012.08.02 13:53:51 -04'00'

Teresa Fryer
CISO and Director, EISG

U.S. DEPARTMENT OF HEALTH AND HUMAN SERVICES

Office of the Secretary

Office of the Assistant Secretary for Administration
Washington, D.C. 20201

May 2, 2012

MEMORANDUM

TO: Operating Division (OPDIV) Chief Information Officers and
Operating Division Chief Information Security Officers

FROM: Daniel Galik D. Galik
HHS Chief Information Security Officer

SUBJECT: HHS Minimum Security Configuration Standards for Departmental Operating Systems and Applications

Information Technology (IT) security configuration baselines establish the minimum system or application security configuration settings needed to ensure secure IT operations across the Department of Health and Human Services (HHS) enterprise. Adhering to security configuration baselines for all IT products employed Department-wide is of critical importance because it ensures that all HHS IT products are configured securely and helps protect sensitive HHS information. Therefore, in the spirit of promoting increased information security, the Department directs all Operating Divisions (OPDIVs) to begin using the security configuration baselines established by the new United States Government Configuration Baselines (USGCB) referenced in the Chief Information Officer (CIO) Council memorandum released on May 7, 2010; and the National Checklist Program (NCP) defined by National Institute of Standards and Technology (NIST) Special Publication (SP) 800-70 Rev 2, *National Checklist Program for IT Products – Guidelines for Checklist Users and Developers*.

The USGCB initiative creates security configuration baselines for IT products widely deployed across Federal agencies (see http://usgcb.nist.gov/ for more information). It is important to note that because the USGCB initiative is new, it may not yet contain baselines for all IT products. If baselines do not exist for a specific IT product, OPDIVs should use the NIST NCP as the approved guide to develop any necessary additional baselines (see http://web.nvd.nist.gov/view/ncp/repository for more information).

OPDIVs are responsible for establishing procedures to test and implement the USGCB and NCP settings within operational environments, and shall make risk-based decisions while customizing the baseline to support functional requirements. All deviations from the USGCB and NCP must be documented in an approved waiver[1], with copies submitted to the Department.

In situations where HHS, USGCB, and NCP guidance does not exist, OPDIVs should collaborate with the HHS Cybersecurity Program and other OPDIVs through the HHS Continuous Monitoring and Risk Scoring (CMRS) working group to establish baselines and communicate industry and vendor best practices.

Based on the comments received by OPDIVs on the latest review of this document, the HHS-specific *Minimum Security Configurations* shall still be valid for the following Operating Systems and Applications:

- HHS FDCC Windows XP Standard
- HHS FDCC Windows Vista Standard
- Blackberry Server
- Websense

The following Minimum Security Configurations that were valid in previous versions of this document have been removed and the Operating Divisions are advised to utilize USGCB and NCP guidance:

- Windows 2003 Server
- Solaris
- HP UX
- Oracle
- Cisco IOS
- Apple OS X
- Apache
- Exchange 2003
- BIND
- MS SQL 2000
- RedHat Linux

The following minimum security configuration standards were removed from the minimum configuration guide as these products are past their end of life and are not acceptable for use on HHS networks:

- Windows NT
- Windows Server 2000
- Windows 2000 Professional

[1] Refer to the *Departmental Security Policy and Standard Waiver Form* on the HHS Cybersecurity Program intranet page.

Your attention to this matter and cooperation in the implementation of this memorandum is greatly appreciated. For questions regarding this guidance or support in following these requirements, please contact HHS Cybersecurity at 202-205-9581 or HHS.Cybersecurity@hhs.gov.