

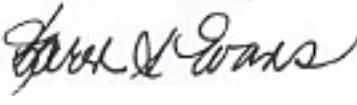


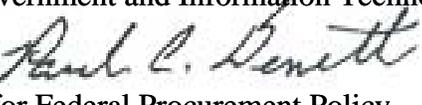
EXECUTIVE OFFICE OF THE PRESIDENT  
OFFICE OF MANAGEMENT AND BUDGET  
WASHINGTON, D.C. 20503

June 1, 2007

M-07-18

MEMORANDUM FOR CHIEF INFORMATION OFFICERS  
CHIEF ACQUISITION OFFICERS

FROM: Karen S. Evans   
Administrator  
Office of E-Government and Information Technology

Paul A. Denett   
Administrator for Federal Procurement Policy

SUBJECT: Ensuring New Acquisitions Include Common Security Configurations

The Office of Management and Budget recently issued policy memorandum M-07-11, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," which stated: "agencies with these operating systems [Windows XP and VISTA] and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008."

This memorandum provides recommended language for your agency to use in solicitations to ensure new acquisitions include these common security configurations and information technology providers certify their products operate effectively using these configurations. Your agency may determine other specifications and/or language is necessary:

- "a) The provider of information technology shall certify applications are fully functional and operate correctly as intended on systems using the Federal Desktop Core Configuration (FDCC). This includes Internet Explorer 7 configured to operate on Windows XP and Vista (in Protected Mode on Vista). For the Windows XP settings, see: [http://csrc.nist.gov/itsec/guidance\\_WinXP.html](http://csrc.nist.gov/itsec/guidance_WinXP.html), and for the Windows Vista settings, see: [http://csrc.nist.gov/itsec/guidance\\_vista.html](http://csrc.nist.gov/itsec/guidance_vista.html).
- b) The standard installation, operation, maintenance, update, and/or patching of software shall not alter the configuration settings from the approved FDCC configuration. The information technology should also use the Windows Installer Service for installation to the default "program files" directory and should be able to silently install and uninstall.
- c) Applications designed for normal end users shall run in the standard user context without elevated system administration privileges."

A number of concurrent activities will further assist your agency's adoption of common security configurations. The National Institute of Standards and Technology (NIST) and the Department of Homeland Security continue to work with Microsoft to establish a virtual machine to provide agencies and information technology providers' access to Windows XP and VISTA images. The images will be pre-configured with the recommended security settings for test and evaluation purposes to help certify applications operate correctly.

Additionally, Part 39 of the Federal Acquisition Regulation (FAR), which requires agencies to include appropriate information technology security policies and requirements when acquiring information technology, will be revised to incorporate requirements for using common security configurations, as appropriate.

More information on how to access the virtual machine and progress to update the FAR will be forthcoming. The Chief Information Officers Council will facilitate the exchange of best practices and lessons learned, and NIST maintains responses to frequently asked questions at: [http://csrc.nist.gov/itsec/guidance\\_WinXP.html#FAQ](http://csrc.nist.gov/itsec/guidance_WinXP.html#FAQ) and [http://csrc.nist.gov/itsec/guidance\\_vista.html#FAQ](http://csrc.nist.gov/itsec/guidance_vista.html#FAQ). Questions concerning agency adoption of the Windows XP and VISTA configurations can be sent to [fisma@omb.eop.gov](mailto:fisma@omb.eop.gov). If you have any questions about this memorandum, please contact Daniel Costello at 202-395-7857.