August 15, 2007   Washington, D.C. 20530

MEMORANDUM FOR BUREAU PROCUREMENT CHIEFS

FROM: Michael H. Allen   *Michael H. Allen*
              Procurement Executive

SUBJECT: DOJ Procurement Guidance Document (PGD) 07- 10
              Ensuring New Acquisitions Include Common Security Configurations

The purpose of this PGD is to advise you of two recent memoranda from the Office of Management and Budget (OMB) concerning the use of common security configurations for Windows Operating Systems. The first one, M-07-11, dated March 22, 2007, "Implementation of Commonly Accepted Security Configurations for Windows Operating Systems," requires agencies with Windows XP and Vista operating systems and/or plans to upgrade to these operating systems to adopt standard security configurations by February 1, 2008. The Department's Chief Information Officer is implementing the requirements of M-07-11 and has submitted a plan to OMB for full implementation.

The second OMB memorandum, M-07-18, dated June 1, 2007, "Ensuring New Acquisitions Include Common Security Configurations," provides recommended language for agencies to use in solicitations to ensure new acquisitions include these common security configurations and that information technology providers certify their products operate effectively using these configurations.

The following language is to be used in all appropriate solicitations and contracts.

(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, and for the Windows Vista settings, see: 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.

Components may use additional specifications as long as they are not in conflict with the above requirements. Please coordinate the use of additional requirements with your computer security office.

The above certification is to be included in all appropriate solicitations immediately. The General Services Administration should be working with all their Group 70 Federal Supply Schedule contractors to have them certify. However, on a case by case basis depending on the size or significance of the acquisition, it may be in our best interests to get the certification when ordering under the FSS contracts. The same case by case decision to acquire the certification would apply to existing task orders and contracts.

Questions on the adoption of the Windows XP and Vista configurations can be sent to fisma@omb.eop.gov. If you have any questions on this PGD 07-10 please call Larry Silvis on (202) 616-3754.