

March 20, 2007

MEMORANDUM FOR CHIEF INFORMATION OFFICERS

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

SUBJECT: Managing Security Risk By Using Common Security Configurations

Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of government information. This memorandum requires your agency to develop plans for using the Microsoft Windows XP and Vista security configurations with an implementation date of no later than February 1, 2008.

As you know, section 3544(b)(2)(D)(iii) of the Federal Information Security Management Act (FISMA) requires agencies to develop minimally acceptable system configuration requirements and ensure compliance with them. Your agency is already required to:

- document in your annual FISMA report the frequency by which you implement system configuration requirements;² and
- use published configurations or be prepared to justify why you are not doing so.

As a model for this effort, the Air Force uses common security configurations for Microsoft Windows XP. These configurations were developed in collaboration with the National Institute of Standards and Technology (NIST), the Department of Homeland Security (DHS), the Defense Information Systems Agency (DISA), the National Security Agency (NSA), and Microsoft. These same organizations recently established common security configurations for Microsoft Vista. With these common security configurations now in place, we have a unique opportunity when using Microsoft Windows XP and acquiring Vista.

Requirements of Agency Plans

Agency plans for Microsoft Windows XP and Vista should be submitted to OMB by May 1, 2007 to fisma@omb.eop.gov and should describe the following items:

- Testing configurations in a non-production environment to identify adverse effects on system functionality;
- Implementing and automating enforcement for using these configurations;
- Restricting administration of these configurations to only authorized professionals;
- Ensuring new acquisitions by June 30, 2007, to include these configurations and require information technology providers to certify their products operate effectively using these configurations;
- Applying Microsoft patches available from DHS when addressing new Windows XP or Vista vulnerabilities;

- Providing NIST documentation of any deviations from these configurations and rationale for doing so; and³
- Ensuring these configurations are incorporated into agency capital planning and investment control processes.

Additional Resources Available to Agencies

By April 20, 2007, OMB in conjunction with DHS and other appropriate agencies will establish a means for information technology providers to obtain software images based on these configurations for test and development purposes. Additionally, the Chief Information Officer's Council will assist and facilitate sharing the common security configurations across the Federal government.

NIST has established a program to develop and maintain common security configurations for many operating systems and applications, and the "Security Content Automation Program" can help your agency use common security configurations.⁴ Additionally, NIST's revisions to Special Publication 800-70, "Security Configuration Checklist Program for IT Products," will provide your agency additional guidance for implementing common security configurations.⁵ For additional information about NIST's programs, please contact Stephen Quinn, at Stephen.Quinn@nist.gov.

We look forward to working with you on this effort to improve Federal information security. If you have questions about this policy, please contact Karen Evans, Administrator, E-Government and Information Technology at (202)395-1181 or at fisma@omb.eop.gov.

¹ The Microsoft Windows XP security configurations are at: http://csrc.nist.gov/itsec/download_WinXP.html, and the Microsoft Vista security configurations are at http://csrc.nist.gov/itsec/guidance_vista.html.

² OMB's FISMA reporting instructions are located at: <http://www.whitehouse.gov/omb/memoranda/fy2006/m06-20.pdf>.

³ Any security configurations developed by your agency for other operating systems should be sent to NIST at checklists@nist.gov. NIST will work with your agency to determine whether they can be published as common security configurations for use by other agencies.

⁴ There are now over 120 common security configurations published on NIST's web site. For more information, see: <http://checklists.nist.gov>. NIST's Computer Security Division website is located at <http://csrc.nist.gov/>. For more information about the security content automation program, see <http://nvd.nist.gov/scap.cfm>.

⁵ NIST Special Publication 800-70, "Security Configuration Checklist Program for IT Products," is located at <http://csrc.nist.gov/checklists/SP800-70-DRAFT.pdf>.