Secure One HHS

OMB 07-11, Implementation of Commonly Accepted Security Configurations for Windows Operating Systems Considerations and Concerns

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Office of Management and Budget Memo 07-11 contains a number of requirements for federal agencies

- Agencies who have Windows XP TM deployed and plan to upgrade to the Vista operating system, are directed to adopt the security configurations developed by the National Institute of Standards and Technology (NIST), the Department of Defense (DoD) and the Department of Homeland Security (DHS)
- Agencies must put in place the proper governance structure with appropriate policies to ensure a very small number of secure configurations are allowed to be used
- Agencies with these operating systems and/or plans to upgrade to these operating systems must adopt these standard security configurations by February 1, 2008
- Agencies are requested to submit their draft implementation plans by May 1, 2007 at fisma@omb.eop.gov

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

An additional memo from OMB for "Managing Security Risk By Using Common Security Configurations" stipulates additional requirements

- Agency are to develop plans for using the Microsoft Windows XP and Vista security configurations with an implementation date of no later than February 1, 2008
- Agency plans for Microsoft Windows XP and Vista should be submitted to OMB by May 1, 2007 to include 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; and
  - Ensuring these configurations are incorporated into agency capital planning and investment control processes

FISMA already requires the use of system configuration baselines and related compliance testing

- Specifically FISMA requires agencies to:
  - document in the agency annual FISMA report the frequency by which you implement system configuration requirements; and
  - use published configurations or be prepared to justify why you are not doing so

- Challenge lies in verifying that secure configurations are implemented and maintained across large enterprises

SECURE ONE HHS
KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Several agencies, including HHS, were already well on the road to compliance with 07-11 when it was released due to forward thinking about security

- In 2006 HHS developed and released minimum configuration requirements for ten different operating systems and applications including Windows XP
- HHS reviews on an annual basis all configuration requirement and adjusts them as needed to increase the security of Department systems
- The annual review process includes identification of emerging operating systems and applications and develops baselines for them as they become available
- We are currently piloting two enterprise solutions for evaluating compliance with configuration standards and will select a final tool later this summer

A number of activities may be required to achieve compliance with OMB 07-11

- Revise and update existing organizational configurations for Windows XP and VISTA
- Distribute the requirements to stakeholders for review and comment to create a high level of acceptance and compliance with the OMB mandated configurations
- Develop an implementation plan for meeting the requirements outlined in OMB 07-11
- Developing internal guidance on OMB 07-11 for distribution with the plan to stakeholders to include organizational level responses

However, there are a number of factors which may limit an organization's ability to achieve compliance with 07-11

- Many organizations do not have existing governance structures and will need to develop them in order to comply
- Tools and technologies for organization wide compliance testing may not be exist in the organization and would need to be purchased and implemented
- The OMB 07-11 configuration requirements may not be compatible with the business activities of the organization and may require significant effort to justify non acceptance or re designing organizational standards and procedures

However, there are a number of factors which may limit an organization's ability to achieve compliance with 07-11 (continued)

- Work will need to be done to incorporated the use of approved secure configurations into capital planning and investment control processes
- Adjustments may be need to existing acquisition agreements in order to ensure that they include these configurations
- Requiring information technology providers to certify their product operates effectively using these configurations may require revision of existing and future contracts
- Patch management tools and processes may need to be acquired and existing ones configured in order to obtain Microsoft patches from DHHS when addressing new Windows XP or Vista vulnerabilities

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

SECURE ONE HHS

KEEP AMERICA'S HEALTH AND HUMAN SERVICES SECURE

Secure One Support
Secureone.hhs@hhs.gov
202-205-9581