US Government Configuration Baseline (USGCB) Highlights

Windows 7 and Internet Explorer 8

The Architecture and Infrastructure Committee's (AIC) Technology Infrastructure Subcommittee (TIS), in conjunction with the National Institute for Standards and Technology (NIST), present the final version of the USGCB settings for Windows 7 and Internet Explorer 8. The USGCB is a further clarification of the Federal Desktop Core Configuration (FDCC); specifically, the USGCB initiative falls within FDCC and comprises the configuration settings component of FDCC.

Key changes from the original FDCC configuration settings include:

- The USGCB is a baseline, which means that all agencies must meet the minimum requirements. USGCB is intended to be the core set of security related configuration settings by which all federal agencies should comply. There is no penalty for more restrictive configurations to meet agency needs. As stated in the May 7th CIO memo[1], "Agencies should make risk based decisions as they customize the baseline for their operational environment and should document and track any changes, including implementation of more secure settings"
- Increased focus on Green IT: The USGCB includes power management settings to save energy, money, and help protect the environment. Computers will go into "sleep" mode after 60 minutes of inactivity. The monitor will go into "sleep" mode after 20 minutes of inactivity. These settings are applicable to AC power and DC or battery power profiles. See the EPA guidance for more information.[2]
- Conditional settings: Configuration settings (i.e. IPv6 and wireless) are included in the USGCB for Windows 7 as conditional settings in recognition that these will only be applicable to some agencies. Only agencies making use of IPv6 or wireless should implement these recommended configuration settings.
- These settings will be harmonized with Windows Vista, XP, and IE 7 where appropriate to ensure consistent baseline according to the FDCC policy.

Key features of the USGCB for Windows 7 and Internet Explorer 8 include:

- Settings that are the result of a collaborative effort between the Department of Defense (DoD), Department of Homeland Security (DHS), NIST, the TIS, and numerous members of the federal information security community who contributed suggestions during the public review process. A result of this collaborative effort is an understanding of the rationale behind each configuration setting.
- Reduced risk of exploit of yet-to-be discovered vulnerabilities as well as current security issues.
- Group Policy and virtual machine disk images to facilitate testing and deployment.
- SCAP Content to support compliance testing and reporting.

Agencies are expected to:

- Implement the Windows 7 and Internet Explorer 8 USGCB settings to achieve a secure and environmentally aware computing environment.
- Follow proper procedures within their organization to fully test prior to deploying USGCB to operational Windows 7 machines.

[1] http://www.cio.gov/Documents/USGCB_Win7IE8_announcement_final.pdf
[2] http://www.energystar.gov/index.cfm?c=power_mgt.pr_power_mgt_users

- Document and track any changes to USGCB settings, to include more restrictive configurations, when customizing the baseline as appropriate to meet site-specific needs.
- Include the application of these settings as part of a comprehensive, well-structured security program.
- Continue to comply with existing mandates including configuration settings, acquisition, and reporting.

Discussion Topic:

- What is an appropriate deadline to establish for agency compliance with USGCB settings for Windows 7 and Internet Explorer 8?