



From FDCC to USGCB

Managing the Transition to a New
Federal Government Security Mandate

TECHNICAL WHITE PAPER

The introduction of new software and applications in use by its employees, combined with a growing number of security threats, has resulted in a new U.S. government mandate, called the United States Government Configuration Baseline (USGCB), designed to ensure that agencies and contractors are adequately protecting their networks.

What is the USGCB? Why should you care? And how can you be sure your agency or organization is covered? The answers to these questions, and more, are discussed in this paper, which shows how to transition from previous network security mandates to the USGCB. This paper also discusses what you need to look for in security solutions to ensure that you're complying with the mandates and improving your organization's security profile.

The Beginnings of Government Security Mandates

The federal government first instituted security guidelines in 2007 with a directive from the Office of Management and Budget (OMB) on the "implementation of commonly accepted security configurations for Windows operating systems." This directive, called the Federal Desktop Core Configuration (FDCC), required agencies to adopt security configurations defined by the National Institute of Standards and Technology (NIST) for Windows XP and Vista operating systems.

The FDCC required that all federal agencies standardize the configuration of about 300 settings on their Windows XP and Vista computers. This effort was intended to strengthen IT security by decreasing the opportunities for hackers to access and exploit government computer systems.

Over time, as Microsoft introduced new software and operating systems, the government needed to update the established security configuration guidelines. In 2010, NIST introduced the USGCB, which was designed to replace the FDCC and expand the baseline configuration guidelines to Windows 7, Windows 7 Firewall and Internet Explorer 8.

The USGCB is a further clarification of the FDCC; specifically, the USGCB initiative constitutes the configuration settings component of the FDCC.

The USGCB is designed not only to address current security issues, but also to reduce the risk of yet-to-be discovered vulnerabilities.¹ In addition, it requires group policy and virtual machine disk images to facilitate testing and deployment, and it requires Security Content Automation Protocol (SCAP) content to support compliance testing and reporting.

USGCB focuses on more than just security. It includes mandates for power-management settings to save energy, reduce costs, protect the environment and comply with executive orders.

The establishment of these baseline configurations, first through FDCC and now through USGCB, has been "one of the most successful government IT programs aimed at helping to increase security, reduce costs, and accelerate the adoption of new government technologies, while creating a more managed desktop environment," according to Microsoft.²

Implementing USGCB

The ultimate responsibility for instituting proper USGCB testing and implementation falls to each individual agency or government contracting organization. These settings were developed and tested on enterprise-connected laptop and desktop computers. Embedded computers, process control systems, and specialized scientific or experimental systems remain outside the scope of the USGCB.

Each agency can also customize the baseline to support its own unique requirements and operational challenges. However, it is important to note that the FDCC-mandated use of SCAP checklists for Windows XP, Vista and Internet Explorer 7 remain in effect until the USGCB checklists are produced for these platforms.

¹ http://www.cio.gov/Documents/USGCB_CIOC091510_final.pdf

² <http://www.microsoft.com/industry/government/solutions/usgcb/default.aspx>

As part of the USGCB, agencies and government contractors are expected to do the following:³

- Implement Windows 7 and Internet Explorer 8 USGCB settings to achieve a secure and environmentally aware computing environment.
- Follow proper procedures within their organizations to fully test before deploying USGCB to operational Windows 7 systems.
- Document and track any changes to USGCB settings, if they implement more restrictive configurations when customizing the baseline 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.

The Value of Establishing a Baseline

Beyond the stated primary goal of improving security, the desktop standardization achieved through established baselines such as the USGCB can provide significant value for an agency, in terms of both IT operations and public-facing functions.⁴ These additional benefits include

- Streamlined management of desktop computers and other devices
- Faster compliance with agency or government requirements and more consistent enforcement of policies
- Seamless and secure access to data and applications—even legacy applications—from any computer
- Reduced energy consumption

How to Ensure Compliance

Although the USGCB sets the baselines that each agency and government contractor is required to adhere to, these organizations need to find a simple yet flexible solution that enables them to maintain the previous FDCC security policies while expanding to include the new mandates. Because of budget constraints, it's not realistic to expect a "forklift upgrade," by which an agency instantly has all new computers using Windows 7 and Internet Explorer 8. The migration could take months, or even years, so both the FDCC and USGCB will be pertinent.

To simplify the process of maintaining the baseline security requirements, users should choose a management solution that meets more than just the basic needs of the mandate. It should offer the flexibility not only to do compliance reporting, but also to build custom reports that can help enhance security and improve productivity. A solution should be capable of documenting changes to the settings and offer customization so that administrators can address exceptions to the regulations or conflicts with existing applications.

Additionally, to minimize management complexities, users should consider an agentless solution. Agentless solutions require no software to be maintained at each computer endpoint—which can be a Herculean effort for agencies with hundreds or thousands of computers in operation. Using agentless solutions, users can reach out to all the endpoints and scan for compliance with the mandates, remediate the problems and produce reports for auditing compliance.

When it comes to reporting, a solution should support XML format for filing USGCB compliance reports, but offer more robust reporting capabilities that can deliver actionable information for an agency's IT staff and administrators.

The USGCB requirements for desktop and laptop computers are just the start of accountability for configuration management. Servers will soon be included in the mandates, so the management, compliance and reporting solution should be able to easily extend to these devices as well.

³ http://www.cio.gov/Documents/USGCB_CIOC091510_final.pdf

⁴ <http://www.microsoft.com/industry/government/solutions/usgcb/default.aspx>

Easing the Transition

As federal agencies and government contractors transition from FDCC to USGCB, they need to ensure that they're adhering to existing mandates while integrating the new ones into their IT management processes.

By implementing a simple, flexible, agentless tool, these organizations' IT staff can easily check compliance of all laptop and desktop endpoints, change the settings on those that do not meet the baseline standards, and collect the data necessary, not only for federal government compliance reports, but also to help improve processes and streamline IT operations.

