GAO

Accountability·Integrity·Reliability

Highlights

Highlights of GAO-10-202, a report to congressional requesters

March 2010

INFORMATION SECURITY

Agencies Need to Implement Federal Desktop Core Configuration Requirements

Why GAO Did This Study

The increase in security incidents and continuing weakness in security controls on information technology systems at federal agencies highlight the continuing need for improved information security. To standardize and strengthen agencies' security, the Office of Management and Budget (OMB), in collaboration with the National Institute of Standards and Technology (NIST), launched the Federal Desktop Core Configuration (FDCC) initiative in 2007.

GAO was asked to (1) identify the goals, objectives, and requirements of the initiative; (2) determine the status of actions federal agencies have taken, or plan to take, to implement the initiative; and (3) identify the benefits, challenges, and lessons learned in implementing this initiative. To accomplish this, GAO reviewed policies, plans, and other documents at the 24 major executive branch agencies; reviewed OMB and NIST guidance and documentation; and interviewed officials.

What GAO Recommends

GAO recommends that OMB, among other things, issue guidance on assessing the risks of deviations and monitoring compliance with FDCC. GAO also recommends that 22 agencies take steps to fully implement FDCC requirements. These agencies generally concurred with GAO's recommendations.

To view the full product, including the scope and methodology, click on GAO-10-202. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

The goals of FDCC are to improve information security and reduce overall information technology operating costs across the federal government by, among other things, providing a baseline level of security through the implementation of a set of standard configuration settings on government-owned desktop and laptop computers (i.e., workstations). To carry out the initiative, OMB required that executive branch agencies take several actions, including: (1) submit an implementation plan to OMB; (2) apply all configuration settings to all applicable workstations by February 2008; (3) document any deviations from the prescribed settings and have them approved by an accrediting authority; (4) acquire a specified NIST-validated tool for monitoring implementation of the settings; (5) ensure that future information technology acquisitions comply with the configuration settings; and (6) submit a status report to NIST.

While agencies have taken actions to implement these requirements, none of the agencies has fully implemented all configuration settings on their applicable workstations. Specifically, most plans submitted to OMB did not address all key implementation activities; none of the agencies implemented all of the prescribed configuration settings on all applicable workstations, though several implemented agency-defined subsets of the settings; several agencies did not fully document their deviations from the settings or establish a process for approving them; six agencies did not acquire and make use of the required tool for monitoring FDCC compliance; many agencies did not incorporate language into contracts to ensure that future information technology acquisitions comply with FDCC; and many agencies did not describe plans for eliminating or mitigating their deviations in their compliance reports to NIST. Until agencies ensure that they are meeting these FDCC requirements, the effectiveness of the initiative will be limited.

FDCC has the potential to increase agencies' information security by requiring stricter security settings on workstations than those that may have been previously in place and standardizing agencies' management of workstations, making it easier to manage changes such as applying updates or patches. In addition, a number of lessons can be learned from the management and implementation of the FDCC initiative which, if considered, could improve the implementation of future versions of FDCC or other configuration efforts. At the same time, agencies face several ongoing challenges in fully complying with FDCC requirements, including retrofitting applications and systems in their existing environments to comply with the settings, assessing the risks associated with deviations, and monitoring workstations to ensure that the settings are applied and functioning properly. As OMB moves forward with the initiative, understanding the lessons learned as well as the ongoing challenges agencies face will be essential in order to ensure the initiative is successful in ensuring public confidence in the confidentiality, integrity, and availability of government information.