October 6, 2011

INFORMATION SECURITY

Additional Guidance Needed to Address Cloud Computing Concerns

GAO Accountability * Integrity * Reliability

Highlights

Highlights of GAO-12-130T, a testimony before the Subcommittee on Cybersecurity, Infrastructure Protection, and Security Technologies, Committee on Homeland Security, House of Representatives

Why GAO Did This Study

Cloud computing, an emerging form of computing where users have access to scalable, on-demand capabilities that are provided through Internet-based technologies, has the potential to provide information technology services more quickly and at a lower cost, but also to introduce information security risks. Accordingly, GAO was asked to testify on the security implications of cloud computing. This testimony describes (1) the information security implications of using cloud computing services in the federal government; (2) GAO's previous reporting on federal efforts and guidance to address cloud computing information security; and (3) GAO recommendations and subsequent actions taken by federal agencies to address federal cloud computing security issues. In preparing this statement, GAO summarized its May 2010 report on cloud computing security and assessed agency actions to implement its recommendations.

What GAO Recommended

GAO is not making additional recommendations at this time beyond the ones made in its 2010 report.

View GAO-12-130T. For more information, contact Gregory C. Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

What GAO Found

Cloud computing has both positive and negative information security implications for federal agencies. Potential information security benefits include the use of automation to expedite the implementation of secure configurations on devices; reduced need to carry data on removable media because of broad network access; and low-cost disaster recovery and data storage. The use of cloud computing can also create numerous information security risks for federal agencies. Specifically, 22 of 24 major federal agencies reported that they were either concerned or very concerned about the potential information security risks associated with cloud computing. Risks include dependence on the security practices and assurances of vendors and the sharing of computing resources. These risks may vary based on the cloud deployment model. Private clouds, whereby the service is set up specifically for one organization, may have a lower threat exposure than public clouds, whereby the service is available to any paying customer. Evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation.

In its 2010 report, GAO noted that governmentwide cloud computing security activities had been undertaken by organizations such as the Office of Management and Budget (OMB), General Services Administration (GSA), and the National Institute of Standards and Technology (NIST); however, significant work remained to be completed. For example, OMB had not yet finished a cloud computing strategy, including how information security issues were to be addressed. GSA had begun a procurement for expanding cloud computing services, but had not yet developed specific plans for establishing a shared information security assessment and authorization process. In addition, although NIST was responsible for establishing information security guidance for federal agencies, it had not yet issued cloud-specific security guidance.

In its report, GAO made several recommendations to address cloud computing security that agencies have taken steps to implement. Specifically, GAO recommended that OMB establish milestones to complete a strategy for federal cloud computing and ensure it addressed information security challenges. OMB subsequently published a strategy which addressed the importance of information security when using cloud computing, but did not fully address several key challenges confronting agencies. GAO also recommended that GSA consider security in its procurement for cloud services, including consideration of a shared assessment and authorization process. GSA has since developed a draft of an assessment and authorization process for systems shared among federal agencies, but the process has not yet been finalized. Finally, GAO recommended that the NIST issue guidance specific to cloud computing security. NIST has issued multiple publications which address such guidance; however, one publication remains in draft, and is not to be finalized until the first quarter of fiscal year 2012.