



Highlights of [GAO-10-513](#), a report to congressional requesters

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 (1) identify the models of cloud computing, (2) identify the information security implications of using cloud computing services in the federal government, and (3) assess federal guidance and efforts to address information security when using cloud computing. To do so, GAO reviewed relevant publications, white papers, and other documentation from federal agencies and industry groups; conducted interviews with representatives from these organizations; and surveyed 24 major federal agencies.

What GAO Recommends

GAO is recommending that the Office of Management and Budget, General Services Administration, and the Department of Commerce take several steps to address cloud computing security, including completion of a strategy, consideration of security in a planned procurement of cloud computing services, and issuance of guidance related to cloud computing security. In comments on a draft of this report, these agencies generally concurred with GAO's recommendations and described efforts under way to implement them.

[View GAO-10-513](#) or [key components](#). For more information, contact Gregory C. Wilshusen (202) 512-6244 or wilshusen@gao.gov.

INFORMATION SECURITY

Federal Guidance Needed to Address Control Issues with Implementing Cloud Computing

What GAO Found

Cloud computing has several service and deployment models. The service models include the provision of infrastructure, computing platforms, and software as a service. The deployment models relate to how the cloud service is provided. They include a private cloud, operated solely for an organization; a community cloud, shared by several organizations; and a public cloud, available to any paying customer.

Cloud computing can both increase and decrease the security of information systems in federal agencies. Potential information security benefits include those related to the use of virtualization, such as faster deployment of patches, and from economies of scale, such as potentially reduced costs for disaster recovery. Risks include dependence on the security practices and assurances of a vendor, dependency on the vendor, and concerns related to sharing of computing resources. However, these risks may vary based on the cloud deployment model. Private clouds may have a lower threat exposure than public clouds, but evaluating this risk requires an examination of the specific security controls in place for the cloud's implementation.

Federal agencies have begun efforts to address information security issues for cloud computing, but key guidance is lacking and efforts remain incomplete. Although individual agencies have identified security measures needed when using cloud computing, they have not always developed corresponding guidance. For example, only nine agencies reported having approved and documented policies and procedures for writing comprehensive agreements with vendors when using cloud computing. Agencies have also identified challenges in implementing existing federal information security guidance and the need to streamline and automate the process of implementing this guidance. These concerns include having a process to assess vendor compliance with government information security requirements and the division of information security responsibilities between the customer and vendor. Furthermore, while several governmentwide cloud computing security initiatives are under way by organizations such as the Office of Management and Budget (OMB) and the General Services Administration (GSA), little has been completed as a result of these efforts. For example, OMB has not yet finished a cloud computing strategy. GSA has begun a procurement for cloud computing services, but has faced challenges in completing the procurement due in part to information security concerns. In addition, while the Department of Commerce's National Institute of Standards and Technology has begun efforts to address cloud computing information security, it has not yet issued cloud-specific security guidance. Until specific guidance and processes are developed to guide agencies in planning for and establishing information security for cloud computing, they may not have effective information security controls in place for cloud computing programs.