July 2010

INFORMATION SECURITY

Government wide Guidance Needed to Assist Agencies in Implementing Cloud Computing

GAO Accountability • Integrity • Reliability

Highlights

Highlights of GAO-10-855T, a testimony before the Committee on Oversight and Government Reform and its Subcommittee on Government Management, Organization, and Procurement, 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, reportedly 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 benefits and risks of moving federal information technology into the cloud. This testimony summarizes the contents of a separate report that is being released today which describes (1) the models of cloud computing, (2) the information security implications of using cloud computing services in the federal government, and (3) federal guidance and efforts to address information security when using cloud computing. In preparing that report, GAO collected and analyzed information from industry groups, private-sector organizations, and 24 major federal agencies.

What GAO Recommends

In the report being released today, GAO recommended that the Office of Management and Budget, the General Services Administration, and the Department of Commerce take 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. These agencies generally agreed with GAO's recommendations.

View GAO-10-855T or key components.
For more information, contact Gregory Wilshusen at (202) 512-6244 or wilshuseng@gao.gov.

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; a public cloud, available to any paying customer; and a hybrid cloud, a composite of deployment models.

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 and automation, broad network access, potential economies of scale, and use of self-service technologies. In addition to benefits, the use of cloud computing can create numerous information security risks for federal agencies. Specifically, 22 of 24 major federal agencies reported that they are 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 a vendor, and the 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. Agencies have also identified challenges in assessing vendor compliance with government information security requirements and clarifying 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 and the General Services Administration, significant work needs to be completed. For example, the Office of Management and Budget has not yet finished a cloud computing strategy, or defined how information security issues will be addressed in this strategy. The General Services Administration has begun a procurement for expanding cloud computing services, but has not yet developed specific plans for establishing a shared information security assessment and authorization process. In addition, while the 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 the 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.