GAO Highlights

CYBERSECURITY

Selected Agencies Need to Better Protect Cloud Data

GAO-26-108443 June 2026

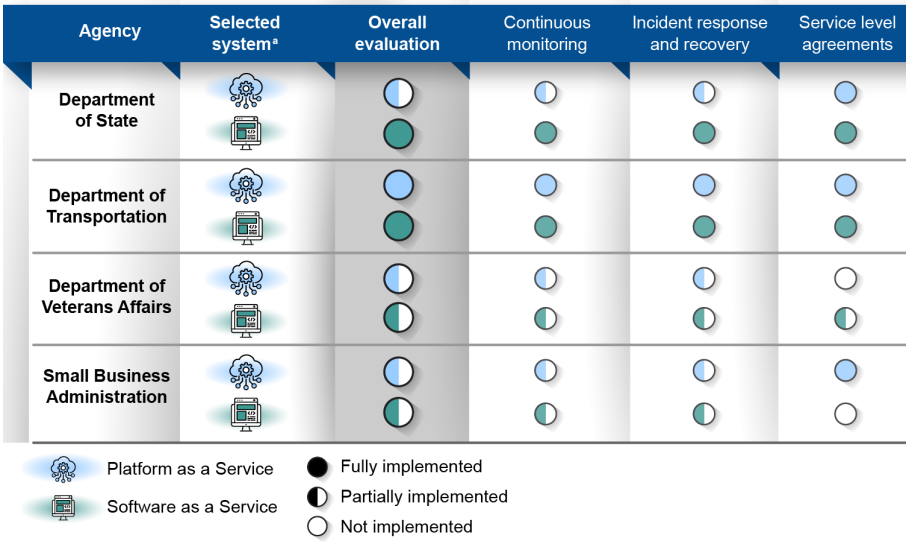
A report to congressional committees

For more information, contact: David B. Hinchman at HinchmanD@gao.gov

What GAO Found

Four selected agencies—the Departments of State, Transportation, Veterans Affairs (VA), and the Small Business Administration (SBA)—varied in their efforts to implement and ensure contractor compliance with three key cloud security practices. Specifically, one agency had fully implemented all three practices for two of its systems and one agency had fully implemented the practices for one of its systems. The agencies partially implemented the practices for the remaining five systems (see figure).

Agencies' Implementation of Key Cloud Security Practices



Sources: GAO analysis of agency documentation; Cetacons/stock.adobe.com (all icons); Agencies (logo). | GAO-26-108443

[a]Due to sensitivity concerns, GAO is not disclosing the names of the selected systems in this report. Systems are identified by their cloud service model.

For example, agencies fully performed continuous monitoring for three of the eight selected systems. Although most of the agencies developed and implemented a plan for continuous monitoring, they did not always review continuous monitoring deliverables from the provider. Agencies fully implemented the practice regarding service level agreements for five out of eight systems. For the remaining three systems, agencies' agreements did not consistently define performance metrics, including how they would be measured and the enforcement mechanisms.

Fully implementing the key practices will support the agencies' efforts to ensure the confidentiality, integrity, and availability of agency information in their cloud systems. For example, without a robust continuous monitoring program, the agencies may have diminished ability to identify and mitigate control deficiencies and emerging threats. Additionally, the agencies may not promptly detect unauthorized access attempts or anomalous activity, leaving critical systems and data exposed to compromise.

Why GAO Did This Study

Federal agencies are faced with the need to accelerate their adoption of cloud services while ensuring the systems that support their missions are secure. Consequently, working with cloud service providers to effectively implement information security controls is a vital part of reducing risks to agency systems.

The Federal Information Security Modernization Act of 2014 includes a provision for GAO to periodically evaluate federal agencies' information security policies and practices. This report assesses the extent to which selected agencies are ensuring contractor compliance with key cloud computing security practices.

To do so, GAO selected four agencies (State, Transportation, VA, SBA) based on their number of cloud authorizations, excluding agencies profiled in recent GAO reports. GAO reviewed two cloud systems at each agency, each of which represented a range of services. GAO administered a standard set of questions, compared documentation on the implementation of key cloud-related practices for each system identified in federal policies and guidance, and interviewed agency officials. GAO rated each agency as having fully, partially, or not implemented each practice for the selected systems.

What GAO Recommends

GAO is making 12 recommendations to State, VA, and the SBA to fully implement key cloud security practices. VA agreed with the recommendations, and State neither agreed nor disagreed. SBA did not provide comments on the report. State and VA also described actions taken or planned to address the recommendations.