GAO Highlights

Highlights of GAO-23-105482, a report to congressional addressees

May 2023

CLOUD SECURITY

Selected Agencies Need to Fully Implement Key Practices

Why GAO Did This Study

Cloud computing provides agencies with potential opportunities to obtain IT services more efficiently; however, if not effectively implemented, it also poses cybersecurity risks. To facilitate the adoption and use of cloud services, the Office of Management and Budget and other federal agencies have issued policies and guidance on key practices that agencies are to implement to ensure the security of agency systems that leverage cloud services (i.e., cloud systems).

This report evaluates the extent to which selected agencies have effectively implemented key cloud security practices. To do so, GAO selected 15 cloud systems across four agencies (Agriculture, DHS, Labor, and Treasury), representing a broad range of services. GAO selected these agencies based on several factors, including the number of reported IT investments leveraging cloud computing. GAO compared relevant agency documentation against six key practices identified in federal policies and guidance. GAO rated each agency as having fully, partially, or not implemented each practice for the selected systems.

What GAO Recommends

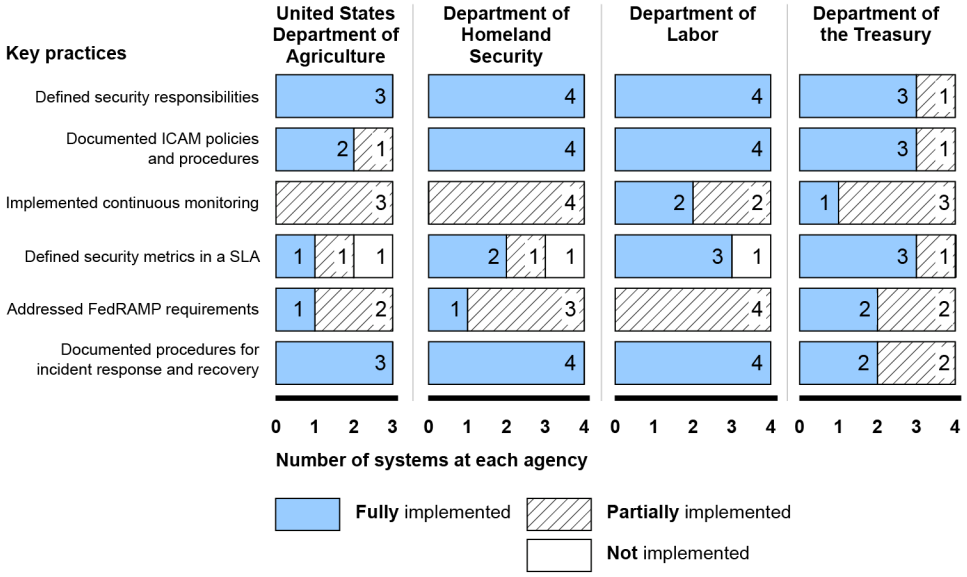
GAO is making 35 recommendations to four agencies to fully implement key cloud security practices. DHS concurred with the recommendations. Agriculture, Labor, and Treasury neither agreed nor disagreed with the recommendations. DHS, Labor, and Treasury described actions taken or planned to address the recommendations.

View GAO-23-105482. For more information, contact David B. Hinchman at (214) 777-5719 or hinchmand@gao.gov, or Brian Bothwell at (202) 512-6888 or bothwellb@gao.gov.

What GAO Found

The four selected agencies—the Departments of Agriculture, Homeland Security (DHS), Labor, and the Treasury—varied in their efforts to implement the six key cloud security practices that GAO evaluated. Specifically, three agencies fully implemented three practices for most or all of their selected systems, while another agency fully implemented four practices for most or all of its systems. However, the agencies partially implemented or did not implement the other practices for the remaining systems (see figure).

Agencies' Implementation of the Key Cloud Security Practices for Each of the Selected Systems



ICAM (Identity, Credential, and Access Management), SLA (service level agreement), FedRAMP (Federal Risk and Authorization Management Program)

Source: GAO analysis of agency data. | GAO-23-105482

For example, the agencies partially implemented the practice regarding continuous monitoring for some or all of the systems. Although the agencies developed a plan for continuous monitoring, they did not always implement their plans. In addition, agencies partially implemented or did not implement the practice regarding service level agreements for some of the systems. Specifically, agencies' service level agreements did not consistently define performance metrics, including how they would be measured, and the enforcement mechanisms.

Agency officials cited several reasons for their varied implementation of the key practices, including acknowledging that they had not documented their efforts to address the requirements. Until these agencies fully implement the cloud security key practices identified in federal policies and guidance, the confidentiality, integrity, and availability of agency information contained in these cloud systems is at increased risk.