



Office of Inspector General

Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2019-IT-C-009, July 17, 2019

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

Findings

The Bureau of Consumer Financial Protection (Bureau) has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the Federal Risk and Authorization Management Program (FedRAMP) cloud systems it uses. However, we found that the process is not yet effective in ensuring that (1) risks are comprehensively assessed prior to deploying new cloud systems, (2) continuous monitoring is performed to identify security control weaknesses after deployment, and (3) electronic media sanitization renders sensitive Bureau data unrecoverable when cloud systems are decommissioned.

Specifically, we found that the Bureau did not perform an agency-specific risk and security controls assessment and grant an authorization to operate for a FedRAMP cloud system supporting a key agency mission. We also found that the Bureau did not ensure that the FedRAMP Project Management Office had an accurate inventory of the cloud systems used by the agency. This inaccurate inventory hindered the Bureau's ability to perform effective continuous monitoring activities and resulted in weaknesses in verifying incident reporting and contingency plan testing processes for cloud service providers. During our fieldwork, the Bureau implemented an automated process to ensure that accurate inventory information was provided to the FedRAMP Project Management Office. We also found that the Bureau can obtain additional assurance that electronic media sanitization activities performed by cloud service providers render sensitive Bureau data unrecoverable.

Recommendations

This report includes three recommendations designed to strengthen the Bureau's life cycle processes for leveraging FedRAMP cloud systems in the areas of risk management, continuous monitoring, and electronic media sanitization. The Bureau concurs with our recommendations and outlined plans to implement them. We will continue to monitor the Bureau's progress in addressing these recommendations as part of future reviews.

Purpose

The Federal Information Security Modernization Act of 2014 requires that we perform an annual independent evaluation of the Bureau's information security program and practices, including testing the effectiveness of security controls for select information systems. Our objective was to determine whether the Bureau has implemented an effective life cycle process for deploying and managing FedRAMP cloud systems used by the agency, including ensuring that effective security controls are implemented.

Background

FedRAMP was established in 2011 to provide federal agencies with a cost-effective, risk-based approach for the adoption and use of cloud computing services. Since its establishment in July 2011, the Bureau has embraced cloud computing as a model to meet its information technology needs in a flexible, scalable manner. The Bureau uses five FedRAMP cloud systems to support various mission and business processes. As part of its technology vision, the Bureau plans to move to a cloud-only information technology infrastructure by 2022.