Office of Inspector General
Board of Governors of the Federal Reserve System
Consumer Financial Protection Bureau

Executive Summary, 2025-IT-C-012, October 31, 2025

2025 Audit of the CFPB's Information Security Program

Findings

The Consumer Financial Protection Bureau's overall information security program has decreased from a level-4 maturity (*managed and measurable*) to a level-2 maturity (*defined*) in fiscal year 2025. We further concluded, based on the results of our determinations of effectiveness in each domain and function, that the CFPB's overall information security program is not effective. We found that the CFPB is not maintaining its authorizations to operate for many systems and is using risk acceptance memorandums without a documented analysis of cybersecurity risks. This issue has been compounded by the loss of contractor resources supporting information security continuous monitoring and testing activities and the departure of agency personnel. As such, the CFPB is unable to maintain an effective level of awareness of security vulnerabilities in its environment. We also found that the CFPB can strengthen its information security program by using cybersecurity profiles to assess, tailor, and prioritize its cybersecurity approach. Specifically, we believe that the use of profiles can help the agency align its cybersecurity program and control structure with the future state of the agency and the sensitive data it maintains.

We further found that, despite these resource and operating constraints, the CFPB was able to take some steps to maintain and strengthen its information security program. For example, the agency updated and formalized processes for responding to potential ransomware incidents and transitioned toward a continuous vetting model for employee background reinvestigations. Additionally, the senior agency information security officer continues to meet with system owners on a weekly basis to manage cybersecurity risks, and the agency is in the process of decommissioning and modernizing legacy technology systems.

Lastly, we continue to identify the use of outdated software on the CFPB's network for which vendors are no longer providing security updates and patches. A key reason for this issue is delays in modernizing, rearchitecting, and retiring legacy applications. We have previously raised this issue and have an open recommendation related to it. As such, we are not including a new recommendation and suggest that management prioritize efforts to reduce the risks resulting from the use of outdated software.

Recommendations

This report includes six new recommendations designed to strengthen the CFPB's information security program in the areas of cybersecurity profiles, security authorizations, and information security continuous monitoring. In response to a draft of our report, the CFPB concurs with our recommendations and notes that the recommendations will

Purpose

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the CFPB. Our specific audit objectives, based on legislative requirements, were to evaluate the effectiveness of the CFPB's (1) security controls and techniques for selected information systems and (2) information security policies, procedures, standards, and guidelines.

Background

FISMA requires each inspector general to conduct an annual independent evaluation of their agency's information security program, practices, and controls for selected systems. The Office of Management and Budget's (OMB) *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* directs inspectors general to evaluate the maturity level (from a low of 1 to a high of 5) of their agency's information security program for fiscal year 2025. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.

enhance the agency's information security program. The agency further outlines actions to address each recommendation. In addition, we are closing three recommendations from our prior years' Federal Information Security Modernization Act of 2014 (FISMA) audit reports. Eight previously made recommendations in the areas of data loss prevention, data classification, flaw remediation, and system/software inventorying remain open. We will continue to monitor the CFPB's progress in addressing our open recommendations as part of future FISMA audits.