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

Executive Summary, 2024-IT-C-019, October 31, 2024

# 2024 Audit of the CFPB's Information Security Program

## Findings

The Consumer Financial Protection Bureau's information security program continues to operate effectively at a level-4 (*managed and measurable*) maturity. We found that the CFPB has taken several steps to strengthen its information security program since our 2023 Federal Information Security Modernization Act of 2014 (FISMA) review. For instance, the CFPB improved its security training program by incorporating threat intelligence to update its workforce on a near-real-time basis.

To ensure that its information security program remains effective, the agency can

- mature data loss prevention (DLP) processes by developing data classification policies and procedures and by configuring its DLP tool accordingly
- strengthen processes to ensure timely remediation of critical and high-risk vulnerabilities
- ensure that system users are periodically reinvestigated to maintain access authorizations and privileges
- improve incident processes to effectively respond to a potential ransomware incident
- strengthen organizational resiliency by conducting a comprehensive test of its continuity of operations plan
- ensure the accuracy of the information in its cybersecurity governance, risk, and compliance tool

In addition, of the seven open recommendations made in our prior years' FISMA audit reports, the CFPB has taken sufficient actions to close four. We will continue to monitor the CFPB's progress in addressing our open recommendations as part of future FISMA audits.

## Recommendations

This report includes eight new recommendations designed to strengthen the CFPB's information security program in the areas of DLP, vulnerability management, personnel security, incident management, contingency planning, and risk management. In its response to a draft of our report, the CFPB concurs with our recommendations and outlines actions to address each recommendation. We will monitor the CFPB's progress in addressing these recommendations as part of future FISMA audits.

## 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 2023–2024 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 2024. OMB notes that level 4 (*managed and measurable*) represents an effective level of security.