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

Executive Summary, 2022-IT-C-014, September 30, 2022

2022 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. Since our review last year, we found that the CFPB has taken steps to strengthen its information security program. For instance, the agency developed its zero trust strategy implementation plan, which outlines the various initiatives and budgetary requirements for the implementation of the CFPB's zero trust architecture (ZTA) by fiscal year 2024. In addition, we found that the CFPB has improved its maturity in the areas of information security continuous monitoring and supply chain risk management.

We identified opportunities to strengthen the CFPB's information security program in the areas of data loss prevention, software asset management, and continuity planning to ensure that its program remains effective. Specifically, we found that the CFPB can strengthen policies and procedures in these areas to ensure that it has repeatable processes in place as it implements its ZTA. We also found that the CFPB can better implement ZTA requirements by ensuring that its new data loss prevention technology is effectively implemented and that an enterprisewide software inventory is developed and maintained. We also found that the CFPB can improve its continuity of operations processes by ensuring that an organizationwide business impact analysis is conducted and maintained.

Finally, the CFPB has taken sufficient actions to close recommendations related to its system authorization and change control processes from our prior Federal Information Security Modernization Act of 2014 (FISMA) audit reports that remained open at the start of this audit. We will update the status of these recommendations in our fall 2022 semiannual report to Congress and continue to monitor the CFPB's progress as part of future FISMA audits.

Recommendations

This report includes six new recommendations designed to strengthen the CFPB's information security program in the areas of data protection and privacy, software asset management, and continuity planning. Our report also includes a matter for management consideration related to the development of procedures for how the CFPB uses a third-party service to monitor vendors' compliance with its cybersecurity requirements. In its response to a draft of our report, the CFPB concurs with our recommendations and outlines actions that have been or will be taken to address them. We will continue to 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 the legislation's requirements, were to evaluate the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

Background

FISMA requires each inspector general to conduct an annual independent evaluation of their agency's information security program, practices, and controls for select systems. The Office of Management and Budget's (OMB) fiscal year 2022 guidance for FISMA reporting 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 across several core areas.

These core areas align to requirements outlined in Executive Order 14028, *Improving the Nation's Cybersecurity*, as well as recent OMB guidance on modernizing federal cybersecurity. The guidance notes that level 4 (*managed and measurable*) represents an effective level of security.