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

Executive Summary, 2017-IT-C-019, October 31, 2017

2017 Audit of the CFPB's Information Security Program

Findings

The Consumer Financial Protection Bureau's (CFPB) overall information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. For instance, the CFPB's information security continuous monitoring process is effective and operating at level 4, with the agency tracking and reporting on performance measures related to supporting activities. In addition, the CFPB employs network access controls to detect unauthorized hardware and has implemented automated patch management tools. These areas are associated with a level-4 maturity.

The CFPB also has opportunities to mature its information security program to ensure that it is effective. Specifically, the agency can strengthen its ongoing efforts to establish an enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels and developing and maintaining an agencywide risk profile. It can also improve configuration monitoring processes for agency databases and applications, multifactor authentication for internal network and systems, and assessments of the effectiveness of security awareness and training activities. Further, the CFPB has opportunities to mature its incident response and contingency planning capabilities to ensure that they are effective.

Finally, the CFPB has taken sufficient action to close one of the four recommendations from our past years' Federal Information Security Modernization Act of 2014 (FISMA) audits that remained open at the start of this audit. Efforts to address the remaining recommendations are underway, and we will continue to monitor the CFPB's progress as part of our future FISMA audits.

Recommendations

Our report includes seven new recommendations designed to strengthen the CFPB's information security program. In its response to our draft report, the CFPB concurs with our recommendations and outlines actions that are underway or will be taken to strengthen the CFPB's information security program. We will continue to monitor the agency's progress in addressing these recommendations as part of future 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 agency Inspector General to conduct an annual independent evaluation of its agency's information security program, practices, and controls for select systems. U.S. Department of Homeland Security guidance for FISMA reporting directs Inspectors General to evaluate the maturity level (from a low of 1 to a high of 5) of their agencies' information security programs across several areas. Level 4 (*managed and measurable*) represents an effective level of security.