Executive Summary:

2016 Audit of the CFPB's Information Security Program

2016-IT-C-012 November 10, 2016

Purpose

To meet our annual Federal Information Security Modernization Act of 2014 (FISMA) reporting responsibilities, we reviewed the information security program and practices of the Consumer Financial Protection Bureau (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 and (2) information security policies, procedures, and practices.

Background

FISMA requires each agency Inspector General (IG) to conduct an annual independent evaluation of the agency's information security program, practices, and controls for select systems. The U.S. Department of Homeland Security has issued guidance to the IGs on FISMA reporting for 2016. The guidance directs the IGs to evaluate the performance of agencies' information security programs across eight domains that are grouped into five function areas: identify, protect, detect, respond, and recover. Also referenced in the guidance is a maturity model for the IGs to use in assessing their agencies' information security continuous monitoring (ISCM) and incident response programs.

Findings

The CFPB continues to mature its information security program to ensure that it is consistent with FISMA requirements. For instance, the CFPB implemented several tools to automate ISCM capabilities, matured its ISCM program from level 1 (*ad hoc*) to level 3 (*consistently implemented*), and strengthened its role-based training program for users with significant security responsibilities. In addition, the CFPB's information security program is generally consistent with seven of eight U.S. Department of Homeland Security information security domains: risk management, contractor systems, configuration management, identity and access management, security and privacy training, ISCM, and incident response. For the remaining domain of contingency planning, the CFPB has not completed an agency-wide business impact analysis to guide its contingency planning activities, nor has it fully updated its continuity of operations plan to reflect the transition of its information technology infrastructure from the U.S. Department of the Treasury.

In addition, while the agency's information security program was generally consistent with requirements outlined in the U.S. Department of Homeland Security's FISMA reporting guidance for IGs in risk management and identity and access management, the CFPB can strengthen controls in those areas to ensure that they are effective. Specifically, the CFPB can strengthen its risk management program by formalizing its insider threat activities and evaluating options to develop an agency-wide insider threat program that leverages planned activities around data loss prevention. Related to the management of insider threat risks, signed rules of behavior documents were not in place for several privileged users who were not consistently resubmitting user access forms to validate the need for their elevated access privileges.

Finally, the CFPB has made further progress in addressing our recommendations from past years' FISMA audit reports. Of 12 total recommendations, 7 remained open at the start of our 2016 FISMA audit. The CFPB has taken sufficient actions to close 6 of the 7 open recommendations.

Recommendations

Our report includes three new recommendations to strengthen the CFPB's information security program: (1) formalize insider threat activities through an agency-wide insider threat program strategy, (2) ensure that user access forms and rules of behavior for privileged users are maintained, and (3) ensure that a business impact analysis is conducted and used to guide contingency planning activities. The Chief Information Officer concurs with our recommendations and has outlined actions that are underway or will be taken to strengthen the CFPB's information security program.