Executive Summary:

2014 Audit of the CFPB's Information Security Program

2014-IT-C-020 November 14, 2014

Purpose

To meet our annual Federal Information Security Management Act of 2002 (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 security controls and techniques as well as compliance by the CFPB with FISMA and related information security policies, procedures, standards, and guidelines.

Background

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program. FISMA also 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 (DHS) has issued guidance to IGs on FISMA reporting for 2014. This guidance directs IGs to evaluate the performance of agencies' information security programs across 11 areas.

Findings

The CFPB continues to take steps to mature its information security program and ensure that it is consistent with the requirements of FISMA. Overall, we found that the CFPB's information security program is consistent with the requirements outlined in DHS's FISMA reporting guidance for IGs in 9 out of 11 areas: information security continuous monitoring (ISCM), configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contractor systems, and security capital planning. Although corrective actions are underway, further improvements are needed in security training and contingency planning.

While we found that the CFPB's information security program was generally consistent with the requirements for ISCM, configuration management, and incident response, we identified opportunities to strengthen these areas through automation and centralization. This year, we found that the Chief Information Officer (CIO) has taken actions to address our 2013 recommendation related to ISCM; however, the CFPB's ISCM program continues to depend on manual, labor-intensive processes. As such, we are closing our 2013 recommendation for ISCM and issuing two additional recommendations to further strengthen the CFPB's ISCM program. In addition, our 2013 FISMA audit report included recommendations to develop and implement (1) an organization-wide configuration management plan and consistent process for patch management, (2) a capability to centrally track and analyze audit logs and security incident information, and (3) a role-based training program. Corrective actions to address these recommendations have not been finalized. As such, we are leaving these recommendations open and will continue to monitor the CFPB's progress in these areas as part of future FISMA audits. We also have a new recommendation for improving configuration management.

Recommendations

Our report includes three new recommendations designed to strengthen the CFPB's ISCM and configuration management practices. We recommend that the CIO (1) fully implement the CFPB's selected automated solution for assessing security controls and analyzing and responding to the results of continuous monitoring activities, and (2) assess the ISCM implementation options and guidance outlined in the *United States Government Concept of Operations for Information Security Continuous Monitoring* and update the CFPB's ISCM strategy, as necessary. We also recommend that the CIO strengthen the CFPB's vulnerability management practices by implementing an automated solution and process to periodically assess and manage database and application-level security configurations.

In response to our report, the CIO concurred with our recommendations and outlined actions that have been taken, are underway, and are planned to strengthen the CFPB's information security program.