Executive Summary:

2013 Audit of the CFPB's Information Security Program

2013-IT-C-020 **December 2, 2013**

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 its agency's information security program and practices. The U.S. Department of Homeland Security (DHS) has issued guidance to IGs on FISMA reporting for 2013. This guidance directs IGs to evaluate the performance of agencies' information security programs across 11 areas.

Findings

Overall, we found that the CFPB has taken multiple steps over the past year to develop, document, and implement an information security program that is consistent with FISMA requirements. The CFPB has also taken several actions to strengthen its information security program in the 11 areas outlined in DHS's 2013 FISMA reporting guidance for IGs. We found that the CFPB's information security program is generally consistent with the requirements outlined in DHS's FISMA reporting guidance for IGs in 6 out of 11 information security areas: identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access management, and contractor systems.

We identified opportunities to improve CFPB's information security program through automation, centralization, and other enhancements to ensure that key DHS requirements for continuous monitoring, configuration management, and security training are met. Further, while we found CFPB's information security program to be generally consistent with DHS's requirements for incident response and reporting, we identified opportunities to strengthen CFPB's incident correlation processes.

We also identified improvements needed in contingency planning for a select system we reviewed. Our findings and recommendations for this system will be communicated under separate, restricted cover. Finally, we noted that the CFPB is taking sufficient actions to establish a security capital planning program, in accordance with the requirements outlined in DHS's FISMA reporting guidance for IGs. We will continue to monitor CFPB's efforts to improve its security capital planning program as part of our future FISMA audits.

Recommendations

Our report includes four recommendations designed to assist the CFPB in strengthening its information security program in the areas of continuous monitoring, configuration management, security training, and incident response and reporting. In a response to a draft of our report, the CFPB's Chief Information Officer concurred with our recommendations and outlined actions that have been taken, are underway, and are planned to strengthen CFPB's information security program.

Access the full report: http://www.consumerfinance.gov/oig/files/CFPB_Audit_Information_Security_FISMA_Dec2013.pdf

For more information, contact the OIG at 202-973-5000 or visit http://www.consumerfinance.gov/oig.