Executive Summary:

2015 Audit of the CFPB's Information Security Program

2015-IT-C-020 **November 13, 2015**

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 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 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 2015. The guidance directs IGs to evaluate the performance of agencies' information security programs across 10 areas. Also referenced in the guidance is a new maturity model for IGs to use in assessing their agencies' information security continuous monitoring (ISCM) programs.

Findings

The CFPB continues to mature its information security program and ensure that it is consistent with the requirements of FISMA. This year, the CFPB completed transitioning its information technology infrastructure and network services from the U.S. Department of the Treasury and assumed most of the operational responsibilities for information security that were previously shared. In addition, 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 9 out of 10 areas: ISCM, configuration management, identity and access management, incident response and reporting, risk management, plan of action and milestones, remote access, contingency planning, and contractor systems. For the remaining area—security training—as we also noted in 2014, we found that the CFPB had not developed and implemented a role-based training program for individuals with key information security responsibilities.

While we found the CFPB's information security program to be consistent with requirements outlined in DHS's FISMA reporting guidance for ISCM, configuration management, incident response, and remote access, we identified opportunities to strengthen controls in these areas. Specifically, we identified improvements needed to mature the CFPB's ISCM program in the areas of people, processes, and technology through greater centralization and automation. In addition, our 2013 and 2014 FISMA audit reports include six recommendations to strengthen the CFPB's ISCM, configuration management, incident response, and security training programs by improving planning, leveraging automation, and increasing centralization. We found that the agency was in the process of taking actions to close these recommendations.

We also identified improvements needed in the CFPB's information security policy and remote access management processes. Specifically, we found that the CFPB had not ensured that its information security policies and procedures were updated in a timely manner to address changing risks and federal requirements. We also found that the CFPB was using an outdated encryption mechanism to secure remote access to its information technology infrastructure.

Recommendations

Our report includes two new recommendations to strengthen the CFPB's information security policy and remote access management processes. These recommendations are designed to (1) ensure that security policies, procedures, and guidance are updated in a timely manner and (2) strengthen the cryptographic mechanism employed for the CFPB's remote access solution in accordance with National Institute of Standards and Technology guidance. In his response to our report, the Chief Information Officer concurs with our recommendations and outlines actions that have been taken, are underway, and are planned to strengthen the CFPB's information security program.