Executive Summary:

Security Control Review of the CFPB's Data Team Complaint Database

2015-IT-C-011 **July 23, 2015**

Purpose

The Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), requires the Office of Inspector General (OIG) to evaluate the effectiveness of the information security controls and techniques for a subset of the agency's information systems, including those provided or managed by another agency, a contractor, or another organization. To meet FISMA requirements, we reviewed the information system security controls for the Consumer Financial Protection Bureau's (CFPB) Data Team (DT) Complaint Database.

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act created the CFPB and directed it to establish a database to facilitate the centralized collection, monitoring, and response to complaints regarding consumer financial products and services. To meet this requirement, the CFPB contracted with several vendors to provide the Consumer Response System (CRS). The DT Complaint Database supports the CRS and is the source of consumer complaint information published on the CFPB's public website. The CFPB's Office of Technology and Innovation is responsible for ensuring that FISMA requirements are met for the database.

Findings

Overall, we found that the CFPB has taken steps to secure the DT Complaint Database in accordance with FISMA and the agency's information security policies and procedures. For example, the CFPB has deployed network-level firewalls and intrusion detection systems for the DT Complaint Database.

However, we identified several control deficiencies related to configuration management, access control, and audit logging and review. Specifically, we identified improvements that are needed in the timely installation of database-level patches, the enforcement of password expiration and user access requirements, and the logging and review of security events. Our report includes seven recommendations to strengthen controls for the DT Complaint Database in these areas.

In response to our report, the Chief Information Officer agreed with our recommendations and outlined actions that have been or will be taken to address our recommendations. We will follow up on the implementation of each recommendation in this report as part of our future audit activities related to the CFPB's continuing implementation of FISMA. Given the sensitivity of information security review work, our reports in this area are generally restricted. Such is the case for this audit report.