Executive Summary:

Security Control Review of the CFPB's Public Website

2017-IT-C-010 **May 22, 2017**

Purpose

The Federal Information Security Modernization Act of 2014 (FISMA) requires the Office of Inspector General 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.

Our audit objective was to evaluate selected security controls for protecting the Consumer Financial Protection Bureau's (CFPB) consumerfinance.gov website from compromise, as well as for compliance with FISMA and other federal and CFPB information security policies, procedures, standards, and guidelines.

Background

The consumerfinance.gov website is critical to the success of the CFPB's mission. Through it, consumers can submit a complaint regarding a financial product and obtain useful information and data regarding financial education resources and the consumer financial marketplace. Financial entities can obtain policy and compliance information related to consumer financial laws and regulations.

Findings

Although the CFPB has taken a number of positive steps to secure its consumerfinance.gov website, several control deficiencies need to be mitigated to protect the website from compromise. Those deficiencies have to do with configuration management, system and information integrity, and contingency planning. If not addressed, these deficiencies could adversely affect the confidentiality, integrity, and availability of consumerfinance.gov and the information it contains.

Our report includes eight recommendations designed to strengthen the security of consumerfinance.gov.

We also identified additional risks for management's continued attention. Those risks relate to system and communications protection, audit and accountability, identification and authentication, system and information integrity, and configuration management. Although the CFPB had recognized these risks prior to our audit, we are including them in our report because they had not been remediated as of the end of our fieldwork. Accordingly, we are not issuing recommendations regarding these risks, but we will continue to monitor the CFPB's progress in mitigating them.

In his response to our report, the Acting Chief Information Officer concurs with our recommendations and outlines actions that have been or will be taken to address them. 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 our information security review work, our reports in this area generally are restricted. Such is the case for this report.