Executive Summary:

Security Control Review of the CFPB's Active Directory Implementation

2017-IT-C-008 April 17, 2017

Purpose

The Federal Information Security Modernization Act of 2014 (FISMA) establishes a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. 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. We conducted this audit to evaluate the administration and security design effectiveness of the Consumer Financial Protection Bureau's (CFPB) Active Directory implementation, including the adequacy of selected security controls for protecting Active Directory, as well as the system's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the CFPB.

Background

Active Directory is used to store information about resources on the network and provide a means of centrally organizing, managing, and controlling access to those resources. The CFPB's Active Directory is hosted within a third-party private cloud environment. This private cloud has been classified by the CFPB as a general support system, and Active Directory is considered to be a key component and an enterprise common service within the private cloud. Among other things, the CFPB uses Active Directory to implement its identity and access management program. As such, Active Directory provides capabilities that help ensure that CFPB users authenticate to information technology resources and have access to only those resources that are required for their job function, a concept referred to as *need to know*.

Findings

Overall, we found that the CFPB is effectively administering and protecting its Active Directory implementation. For example, the CFPB has established a patching and vulnerability scanning process to ensure that the Active Directory infrastructure is maintained with up-to-date configurations. In addition, the CFPB uses tools to log and monitor the activities occurring within Active Directory. We found, however, that the CFPB can strengthen Active Directory controls in the areas of identity and access management and risk management. In addition, as noted in our *2016 Audit of the CFPB's Information Security Program*, we report that improvements are needed in the management of access agreements for Active Directory users.

Our report includes one recommendation and one item for management's consideration. In his response to our report, the Chief Information Officer concurs with our recommendation and outlines actions that have been taken to address it. We will follow up on the implementation of the 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.