



Office of Inspector General

Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2018-IT-C-012R, June 27, 2018

Security Control Review of the Bureau's Mosaic System

Findings

Overall, we found that the security controls we tested for the Mosaic system were operating effectively. Further, specific components of the planning, development, and delivery processes used for the system, as they relate to the Bureau of Consumer Financial Protection's (Bureau) risk management program, were performed effectively. For instance, we found that controls related to continuous monitoring, vulnerability scanning and remediation, and system and information integrity were operating effectively. Further, the Bureau developed a business case, which included an analysis of the benefits and risks, prior to implementing Mosaic. However, we found that the Bureau can strengthen controls in the area of identity and access management to ensure that the security control environment for Mosaic remains effective.

Recommendation

Our report includes one recommendation in the area of identity and access management controls for Mosaic. In its response to our draft report, the Bureau concurs with our recommendation and outlines actions that are underway or will be taken to strengthen identity and access management controls for Mosaic.

In addition, our report includes matters for management's consideration in the areas of audit and accountability, contingency planning, and configuration management. Because we made recommendations in previous audit reports, management actions have been taken, or compensating controls are in place, we are not making formal recommendations in these areas. We will follow up on the implementation of the recommendation and each matter for consideration in our report as part of our future audit activities.

Given the sensitivity of information security review work, our reports in this area are generally restricted. Such is the case for this audit report.

Purpose

The Federal Information Security Modernization Act of 2014 (FISMA) requires that we perform an annual independent evaluation of the Bureau's information security program and practices. Specifically, FISMA requires that we test the effectiveness of the agency's information security policies, procedures, and practices for select information systems. We conducted this audit to evaluate the effectiveness of specific (1) security controls for the Mosaic system and (2) components of the planning, development, and delivery processes used for the system as they relate to the Bureau's risk management program.

Background

The Dodd-Frank Wall Street Reform and Consumer Protection Act created the Bureau and required it to establish a database to facilitate the centralized collection and monitoring of and response to complaints regarding consumer financial products and services. To meet these requirements, the Bureau established the RightNow Consumer Response System, which was replaced in 2017 with Mosaic. Mosaic is a public-facing web application running on a cloud-based platform-as-a-service. In addition to managing consumer complaints, the system provides the Bureau with enhanced services and tools related to workforce and resource management; entity boarding; and the creation and management of investigative records, company ratings, and surveys.