Executive Summary:

Security Control Review of the Board's Active Directory Implementation

2016-IT-B-008 **May 11, 2016**

Purpose

The Federal Information Security Modernization Act of 2014 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 the administration and security design effectiveness of the Active Directory operating environment implemented at the Board of Governors of the Federal Reserve System (Board).

Background

The Board uses Active Directory to manage all elements of its network, including desktops, servers, groups, users, domains, security policies, and any type of user-defined and computer-defined objects. The Board manages and limits access to information systems to authorized users, processes acting on the behalf of users, or devices (including other information systems). It also controls the types of transactions and functions that authorized users are permitted to exercise. A secure Active Directory operating environment is essential to ensuring the confidentiality, integrity, and availability of Board systems and data.

Findings

Overall, we found that the Board is effectively administering and protecting the Active Directory infrastructure. For example, the Board has established a rigorous patching and vulnerability scanning process to ensure that the Active Directory infrastructure is maintained with the most up-to-date configurations. In addition, the Board uses tools to log and monitor the activities occurring in Active Directory. However, we found that the Board can strengthen Active Directory controls in the areas of risk management, continuous monitoring, user group management, contractor account management, and system documentation. Our report includes 10 recommendations to address these Active Directory–related findings. In its response to our draft report, management generally concurs with our recommendations.

In addition, we identified a risk for management's continued attention related to transport layer security. Although the Board has recognized this risk in a plan of action and milestones, we are including the issue in our report because it had not been remediated as of the end of our fieldwork.

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