Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

Executive Summary, 2018-IT-B-019R, November 5, 2018

Evaluation of the Board's Implementation of Splunk

Finding

Overall, we found that the Board of Governors of the Federal Reserve System's (Board) implementation of Splunk generally adheres to security best practices. For example, we found that Splunk forwarders are consistently installed on Board devices and that dashboards have been developed and implemented to monitor and validate that the agency's devices are forwarding data to Splunk correctly. However, we have identified an opportunity to strengthen controls in the area of risk management.

Recommendation

Our report includes one recommendation to strengthen the security of the Board's implementation of the Splunk tool as well as three matters for management's consideration related to Splunk's account management, annual access validation process, and use of self-signed certificates. In its response to our draft report, the Board concurs with our recommendation and outlines corrective actions to address the issues we identified. We will follow up on the implementation of our recommendation and other matters in this report as part of our future audit and evaluation activities.

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

Purpose

Our objective was to evaluate the Board's implementation of the Splunk system in accordance with security best practices as well as the system's compliance with the Federal Information Security Modernization Act of 2014 and the Board's information security policies, procedures, standards, and guidelines.

Background

Log collection and analysis plays a critical role in maintaining a secure and reliable enterprise. One challenge associated with log management that many organizations face is effectively balancing limited log management resources with a continuous supply of log data. Security information and event management (SIEM) software is a relatively new type of centralized logging software that has one or more log servers to perform log analysis and one or more database servers to store the logs.

Splunk is the primary SIEM application used at the Board for audit log collection and analysis. Splunk allows stakeholders throughout the Board to search across logs that are appropriate and applicable to the activities that fall under their purview. Further, the tool provides stakeholders with a framework of dashboards that use automated search and alert capabilities designed to help them meet operational objectives and compliance requirements. When a broader picture is necessary, Splunk also allows groups of data to be combined to correlate events across diverse datasets.