Executive Summary:

The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing

2017-IT-B-009 **April 17, 2017**

Purpose

The Office of Inspector General conducted this evaluation to assess the Board of Governors of the Federal Reserve System's (Board) cybersecurity examination approach and determine whether it is providing effective oversight of financial institutions' information security controls and cybersecurity risks for select oversight areas. Specifically, this evaluation included an assessment of (1) the Board's current cybersecurity oversight approach and governance structure, (2) the current examination practices for financial market utilities and multiregional data processing servicer (MDPS) firms for which the Board has oversight responsibilities, and (3) the Board's ongoing initiative for the future state of cybersecurity oversight. Our scope did not include an assessment of the cybersecurity examination practices for other Board-supervised entities.

Background

Over the past several years, the number and sophistication of cybersecurity threats to the financial sector have increased dramatically. A 2016 report published by Verizon Communications, Inc., on confirmed data and cybersecurity breaches around the world indicates that breaches in the financial industry were the third-most frequent, behind only the public sector and the entertainment industry. As financial institutions have continued to adopt internet-based systems to conduct business, the risks associated with cybersecurity have become more prevalent. In its annual reports to Congress for the past 5 years, the Financial Stability Oversight Council has identified cybersecurity as an area of major concern for companies and governments around the world. Accordingly, cybersecurity threats remain an area of significant focus for both financial institutions and federal financial regulators, as these threats can create significant operational risk, disrupt critical services, and ultimately affect financial stability. As the potential systemic risk of cybersecurity issues continues to increase and evolve, it will be critical for financial institutions and regulators to consider and prepare for the potential effects of significant cybersecurity attacks.

Findings

We identified opportunities for the Division of Supervision and Regulation (S&R) to enhance its approach to cybersecurity supervision as it continues to implement its multiyear, future-state cybersecurity oversight program. Specifically, we found that S&R could improve the oversight of MDPS firms by (1) enforcing the reporting requirement in the Bank Service Company Act for financial institutions to notify their primary regulator of new service relationships within 30 days, (2) considering the implementation of an enhanced governance structure for these firms, (3) providing additional guidance to examination teams on the supervisory expectations for these firms, and (4) ensuring that S&R's intelligence and incident management function is aware of the technologies used by MDPS firms. Further, we identified opportunities to improve the recruiting, retention, tracking, and succession planning of cybersecurity resources in alignment with the Board's strategic plan, as well as opportunities to enhance the communication of cybersecurity-related risks.

Recommendations

Our report contains recommendations designed to enhance several components of S&R's approach to cybersecurity supervision. In its response to our draft report, the Board concurs with our recommendations and outlines actions that have been taken or will be implemented to address our recommendations.