ICBA
INDEPENDENT COMMUNITY BANKERS of AMERICA®
www.icba.org

Board of Governors of the Federal Reserve System, Office of Inspector General evaluation report, "The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing."

MAY 2017

Contact Information:
Jeremy Dalpiaz
AVP, Cyber and Data Security Policy
Jeremy.Dalpiaz@icba.org

Board of Governors of the Federal Reserve System Office of Inspector General evaluation report, "The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing."

I. BACKGROUND

A recent evaluation report from the Office of Inspector General ("OIG") for the Board of Governors of the Federal Reserve System ("Board"), entitled "The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing,"[1] ("Report") highlights improvements the Board could make in their oversight of third parties. Responding to the report, the Board agreed with the recommendations of the OIG.

Third parties play an important role in the everyday affairs of financial institutions of all sizes. In 1962, Congress passed the Bank Company Service Act,[2] which provides authority to the federal banking regulators – the Board, Federal Deposit Insurance Corporation ("FDIC") and the Office of the Comptroller of the Currency ("OCC") - to examine bank service companies performing key services to the same extent as if a bank performed the services itself on its own premises. The Federal Financial Institutions Examination Council ("FFIEC") established the Multiregional Data Processing Servicers ("MDPS") program to examine firms that process mission-critical applications for a large number of financial institutions regulated by more than one agency or provide services in multiple locations through the country. These are generally the largest technology service providers ("TSP" or "TSPs") selected for special monitoring and interagency supervision by the federal banking agencies.

The Board examines financial institutions on cybersecurity through both examination and non-examination activities. The FFIEC IT Handbook provides guidance to examiners on how to assess the level of security risk to a financial institution's information systems and provides a framework for assessing the adequacy of an information security program's integration into overall risk management. Non-examination activities are designed to provide an understanding of the institution, its risk profile and associated policies and practices.

In 2015, the Board's Division of Supervision and Regulation launched a multi-year program known as the Cybersecurity Program Group (CPG) to improve and further develop the Board's cybersecurity oversight program of the largest and systematically important financial institutions. This initiative was established to issue cybersecurity risk policy and set expectations for financial institutions, develop examiner supervisory programs, build a cybersecurity surveillance and risk analysis infrastructure, to increase cybersecurity training and assign examiners to institutions with the most risk, and to implement robust continuous monitoring of cybersecurity risk-management program effectiveness at financial institutions.

[1] Board of Governors of the Federal Reserve System. Office of Inspector General. Evaluation Report 2017-IT-B-009. 17 April 2017. https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-apr2017.htm.
[2] See 12 USC 1867 *et. seq.* available at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap18-sec1867.pdf.

II. OVERVIEW

The objective of the OIG's Report was to assess the Board's cybersecurity examination approach and determine whether it is providing effective oversight of financial institutions' information security controls and cybersecurity risk for select oversight areas including an assessment of:

- The Board's current cybersecurity oversight approach and governance structure;
- The current examination practices for financial market utilities (FMUs) and multiregional data processing services (MDPS) firms for which the Board has oversight responsibilities; and
- The Board's ongoing initiative for the future state of cybersecurity oversight.

The OIG provided analysis on three findings:

- Opportunities exist to further enhance the oversight of multiregional data processing services;
- The Board can better manage human capital associated with its cybersecurity resources; and
- Cybersecurity and information technology risk would benefit from enhanced visibility and focus.

Applicability to Community Banks:

Community banks should ensure they notify their primary Federal regulator of the existence of a vendor service relationship within 30 days of entering into a contract or a vendor performing a service, whichever comes first.

III. SUMMARY

To achieve the OIG's objective, their review focused on current-state cybersecurity supervision activities on FMU and MDPS firms primarily due to their size, the critical nature of the services they provide to financial institutions, as well as their interdependence with the rest of the financial system. The sample included two portfolios. The first was from the Federal Reserve Bank of New York, which conducted 25 percent of the MDPS exams led by the Board in 2014 and the second was the Federal Reserve Bank of Atlanta because it also conducted 25 percent of the MDPS exams led by the Board in 2014.

The scope of the OIG's evaluation included:

- Governance of the Board's cybersecurity oversight program;
- The project management of the Board's future-state Cybersecurity Program Group (CPG) initiatives; and
- The examination work performed for two of the Board's supervision portfolios: financial market utilities (FMUs) and MDPS firms.

Based on their review, the OIG had three findings, which are detailed below.

Finding 1: Opportunities Exist to Further Enhance the Oversight of Multiregional Data Processing Servicers

Under this finding, the OIG recommended that the Board:

-Reiterate to financial institutions the requirement to notify their primary regulator of the existence of new service relationships, and develop a process to periodically reconcile and refresh the listing of MDPS firms and TSPs.

The Bank Company Service Act ("BCSA") requires that financial institutions notify their primary Federal regulator of the existence of a vendor service relationship within 30 days of entering into a contract or a vendor performing a service, whichever comes first.[3] The OIG found the Board is not enforcing this requirement. However, the Report, also found that the unclear definition of "product" and "service" blurs the line as to whether the Board has oversight responsibilities over some vendors. The OIG recommends more clarity in the definition of "service relationship".

-Evaluate options for enhancing the oversight of MDPS firms and TSPs and based on this assessment, identify and implement an enhanced governance structure for supervision of these entities.

The Report noted a specific oversight and governance structure for MDPS firms, despite their size and importance within the financial system as well as their selection for special monitoring and interagency supervision by the Board, FDIC and the OCC. The banking agencies have identified 15 firms with the MDPS designation. The Board may not be fully aware of the universe of TSPs and MDPS firms, given its lack of enforcement of the 30-day reporting requirement under the BCSA.

- Work with other federal banking agencies and the Board's Legal Division, as appropriate, to provide clarification and guidance to examination teams regarding the identification of service relationships and expectations for supervising MDPS firms and TSPs.

The OIG report states that examiners do not have current guidance from the Board, despite the authority granted under the BCSA to issue such regulations and orders, on how to interpret the BSCA in today's environment. As a result, there is lack of guidance which may cause confusion for supervisory staff regarding the types of services that should be examined under the law, potentially affecting the adequacy of cybersecurity supervision.

-Establish a process to document the IT systems being used at the MDPS firms and TSPs and ensure that the Cybersecurity Analytics Support Team ("CAST") is aware of this information so it can provide relevant cybersecurity alerts to supervisory teams.

The Cybersecurity Program Groups Intelligence and Incident Management Workstream developed a Cybersecurity Analytics Support Team (CAST), which is intended to provide cybersecurity intelligence and incident information to S&R regarding recent cybersecurity alerts and attacks. CAST maintains information about the software and hardware inventories for financial institutions overseen by the Board, so that in the event of a cybersecurity alert or incident, notification can be made to the supervisory teams overseeing organizations. However, the Report found that CAST is not fully aware of the technologies used by the MDPS firms.

[3] See 12 USC 1867(c)(2) available at https://www.gpo.gov/fdsys/pkg/USCODE-2010-title12/pdf/USCODE-2010-title12-chap18-sec1867.pdf.

In response to the four recommendations under this Finding, the Board agreed with recommendations and noted it is currently working on a high priority initiative to develop and implement an integrated, nationally coordinated program for IT supervision that includes enhancing the oversight of these firms. The Board will work with other federal banking regulators in developing additional guidance on the identification of service providers and supervisory expectations, as well as notify financial institutions of the reporting requirements for new service provider relationships. The Board notes it will also work with other federal banking regulators to develop a process for collecting information about service provider relationships and periodically refresh the list of significant service provides. Additionally, S&R will work with other federal banking regulators and CAST to establish a process that identifies the technologies used by MDPS firms.

Finding 2: The Board Can Better Manage Human Capital Associated with Its Cybersecurity Resources

Three recommendations were made by the OIG in this area:

- Develop detailed recruitment, retention, and succession plans to ensure an agile, diverse, and highly qualified cybersecurity workforce;
- Evaluate the current allocation of cybersecurity resources throughout the Board and the System to ensure that resource dependencies are accounted for and mitigated, as necessary; and
- Ensure that effective and repeatable processes are implemented to track cybersecurity resources in alignment with the Board's and the supervision functions strategic plans.

Within the Report, the OIG notes that recruitment of cybersecurity personnel has been a challenge, not only at the Board, but within the federal government, as well. In its response, the Board agreed with the recommendations and noted they are implementing initiatives to recruit cybersecurity examiners and analyst positions; they have also requested an exception from a federal government hiring freeze announced in January 2017.

Finding 3: Cybersecurity and IT Risk Would Benefit from Enhanced Visibility and Focus

The final recommendation by the OIG is that the Director of S&R:

- Evaluate the process by which critical IT and cybersecurity risk issues across portfolios are communicated to relevant Board and System supervision personnel and develop a plan to communicate these risks periodically.

In 2014, S&R issued an Advisory letter, AD Letter 14-10, "Enhancing Supervisory Risk Identification, Monitoring and Mitigation," which highlighted that risk identification and monitoring in the Federal Reserve System involves many parties, including system management groups, the surveillance function, Reserve Banks' risk structures, Federal Reserve System risk coordinators, affinity groups and others. One of the directives of the Advisory Letter was to implement a System Risk Council to analyze risk information and develop recommendations to the S&R policy function. While the Risk Council receives various reports, the Report found that there is no formalized plan to regularly communicate these results to other relevant personnel, including System supervision personnel responsible for cybersecurity oversight.

Management agreed with the recommendation and noted that the Risk Council is taking steps to present cybersecurity risks as a standalone topic at a minimum once, if not twice, a year to ensure that the council, as well as all significant Federal Reserve-supervised service providers, are fully informed of all cybersecurity risk across portfolios.