OFFICE OF INSPECTOR GENERAL

Evaluation Report 2017-IT-B-009

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

April 17, 2017

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

Report Contributors

Andrew Gibson, OIG Manager
Laura Shakarji, OIG Manager
Joshua Dieckert, Project Lead
Rebecca Kenyon, IT Auditor
Michael Olukoya, Auditor
Eric Shapiro, Auditor
Brent Melson, Senior OIG Manager
Michael VanHuysen, Senior OIG Manager
Peter Sheridan, Assistant Inspector General for Information Technology
Melissa Heist, Associate Inspector General for Audits and Evaluations

Abbreviations

AD Letter	Advisory Letter
Board	Board of Governors of the Federal Reserve System
CAST	Cybersecurity Analytics Support Team
CPG	Cybersecurity Program Group
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FFIEC	Federal Financial Institutions Examination Council
FMU	financial market utility
Framework	Cybersecurity Framework
FRB Atlanta	Federal Reserve Bank of Atlanta
FRB New York	Federal Reserve Bank of New York
FSOC	Financial Stability Oversight Council
HPI	high-priority initiative
IT	information technology
IT Handbook	*Federal Financial Institutions Examination Council Information Technology Examination Handbook*
LISCC	Large Institution Supervision Coordinating Committee
MDPS	multiregional data processing servicer
OIG	Office of Inspector General
PFMI	*Principles for Financial Market Infrastructures*
S&R	Division of Supervision and Regulation
System	Federal Reserve System
TSP	technology service provider

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.

Summary of Recommendations, OIG Report 2017-IT-B-009

Recommendation number	Page	Recommendation	Responsible office
1	10	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 multiregional data processing servicer firms and technology service providers.	Division of Supervision and Regulation
2	10	Evaluate options for enhancing the oversight of multiregional data processing servicer firms and technology service providers, and based on this assessment, identify and implement an enhanced governance structure for supervision of these entities.	Division of Supervision and Regulation
3	10	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 the expectations for supervising multiregional data processing servicer firms and technology service providers.	Division of Supervision and Regulation
4	10	Establish a process to document the information technology systems being used at the multiregional data processing servicer firms and technology service providers, and ensure that the Cybersecurity Analytics Support Team is aware of this information so it can provide relevant cybersecurity alerts to supervisory teams.	Division of Supervision and Regulation
5	13	Develop detailed recruitment, retention, and succession plans to ensure an agile, diverse, and highly qualified cybersecurity workforce.	Division of Supervision and Regulation
6	13	Evaluate the current allocation of cybersecurity resources throughout the Board and the Federal Reserve System to ensure that resource dependencies are accounted for and mitigated, as necessary.	Division of Supervision and Regulation
7	14	Ensure that effective and repeatable processes are implemented to track cybersecurity resources in alignment with the Board's and the supervision function's strategic plans.	Division of Supervision and Regulation
8	16	Evaluate the process by which critical information technology and cybersecurity risk issues across portfolios are communicated to relevant Board and Federal Reserve System supervision personnel, and develop a plan to communicate these risks periodically.	Division of Supervision and Regulation

Office of Inspector General

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

April 17, 2017

MEMORANDUM

TO: Michael S. Gibson
Director, Division of Supervision and Regulation
Board of Governors of the Federal Reserve System

Matthew J. Eichner
Director, Division of Reserve Bank Operations and Payment Systems
Board of Governors of the Federal Reserve System

FROM: Peter Sheridan
Assistant Inspector General for Information Technology

Melissa Heist
Associate Inspector General for Audits and Evaluations

SUBJECT: OIG Report 2017-IT-B-009: *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing*

The Office of Inspector General has completed its report on the subject evaluation. We conducted this evaluation to assess the Board's cybersecurity examination approach and determine whether it is providing effective oversight of financial institutions' information security controls and cybersecurity 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 servicers for which the Board has oversight responsibilities, and (3) the Board's ongoing initiative for the future state of cybersecurity oversight.

We provided you with a draft of our report for review and comment. In your response, you outline actions that have been taken or will be implemented to address our recommendations. We have included your response as appendix A to our report.

We appreciate the cooperation that we received from the Division of Supervision and Regulation and the Division of Reserve Bank Operations and Payment Systems. Please contact either of us if you would like to discuss this report or any related issues.

cc: Donald V. Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Arthur Lindo, Senior Associate Director, Division of Supervision and Regulation
Stuart Sperry, Deputy Associate Director, Division of Reserve Bank Operations and Payment Systems
Steve Bernard, Acting Chief Financial Officer and Acting Director, Division of Financial Management

Contents

Introduction

Objective

Our objective was to evaluate 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 for select oversight areas. 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 (FMUs) 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, such as domestic or foreign bank holding companies, large banking organizations, or community banking organizations. Our scope also did not include SWIFT[1] or FedWire.[2] Additional details on our scope and methodology are described within the Background section.

Background

The Current State of Cybersecurity in the Financial Sector

Over the past several years, the number and sophistication of cybersecurity threats to the financial sector have increased dramatically. As financial institutions have continued to adopt internet-based systems to conduct business, the risks associated with cybersecurity have become more prevalent. Verizon Communications, Inc., publishes an annual report on confirmed data and cybersecurity breaches around the world. Its 2016 report[3] indicates that breaches in the financial industry were the third-most frequent, behind only the public sector and the entertainment industry.

In response to these expanding cybersecurity risks, both public- and private-sector organizations are making efforts to enhance cybersecurity risk-management and resiliency standards. For example, the National Institute of Standards and Technology developed a risk-based Cybersecurity Framework (Framework)[4] to serve as a set of industry standards and best practices to help organizations manage cybersecurity risks. While not a one-size-fits-all approach, the

1. SWIFT, or the Society for Worldwide Interbank Financial Telecommunication, provides messaging services and software to financial entities.

2. FedWire is a wire transfer service that banks and businesses use to send and receive same-day payments.

3. Verizon, *2016 Data Breach Investigations Report*, available at http://www.verizonenterprise.com/verizon-insights-lab/dbir/2016.

4. More information on this framework is available at https://www.nist.gov/cyberframework.

Framework is designed to provide organizations, regardless of size, cybersecurity sophistication, or vulnerability to cybersecurity risk, with standards, guidelines, and practices to address these evolving threats.

Consistent with the Framework, the Federal Financial Institutions Examination Council (FFIEC)[5] has developed a Cybersecurity Assessment Tool to help institutions identify their risks and determine their cybersecurity maturity level. The FFIEC is encouraging the use of this self-assessment tool, which provides institutions with a repeatable and measureable process to inform management of their risks and cybersecurity preparedness. The FFIEC has also recently updated its *Federal Financial Institutions Examination Council Information Technology Examination Handbook* (IT Handbook)[6] to promote consistent information technology (IT) examination practices across federal banking regulators. The IT Handbook is composed of a series of booklets on a variety of IT examination topics, such as business continuity planning, information security, and the supervision of technology service providers (TSPs).

The financial crisis of 2007 to 2009 evidenced the challenges presented by the interconnectedness of participants in the financial system. From trading systems to settlement activities, these complex and sometimes opaque relationships continue to pose a risk to financial stability. In its annual reports to Congress for the past 5 years,[7] the Financial Stability Oversight Council (FSOC)[8] has identified cybersecurity as an area of major concern for companies and governments around the world. Accordingly, cybersecurity remains 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 threats 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.

The Role of the Board in Supervision

The supervision of financial institutions is one of the Board's principal functions in seeking to ensure that the nation's financial system operates in a safe and sound manner. As part of its supervisory activities, the Board has oversight authority and responsibility for several segments

5. The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms and to make recommendations to promote uniformity in the supervision of financial institutions supervised by federal financial regulators, such as the Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau.

6. The IT Handbook is available at http://ithandbook.ffiec.gov/it-booklets.aspx.

7. FSOC's annual reports to Congress are available at https://www.treasury.gov/initiatives/fsoc/studies-reports/Pages/2016-Annual-Report.aspx.

8. Established under the Dodd-Frank Wall Street Reform and Consumer Protection Act, FSOC is charged with identifying risks to the financial stability of the United States, promoting market discipline, and responding to emerging risks to the stability of the U.S. financial system.

of the U.S. financial industry, and it delegates some of its authority[9] to execute this responsibility to the Federal Reserve Banks.[10] Specifically, the Board has supervisory oversight of bank holding companies, the U.S. operations of certain foreign banks, nonbank financial institutions that are designated as systemically important by FSOC, and state-chartered banks that are members of the Federal Reserve System (System). In addition, the Board supervises FMUs, which participate in the payment, clearance, and settlement activities that compose the nation's financial infrastructure. The Board also provides oversight to the firms that provide technology services to supervised entities, the largest of which are known as MDPS firms.

Financial Market Utilities

FMUs are multilateral systems that provide the essential infrastructure for the transfer, clearance, and settlement of payments, securities, and other financial transactions among financial institutions or between financial institutions and the U.S. financial system. FMUs that conduct or support multilateral payment, clearing, and settlement activities may reduce risks for their participants and the broader financial system, but such utilities may also concentrate and create new risks and thus must be well designed and operated in a safe and sound manner. In accordance with title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act), FSOC may designate those FMUs that it determines are, or are likely to become, systemically important. To date, FSOC has designated eight FMUs as systemically important, and under title VIII of the Dodd-Frank Act, the Board is the supervisory agency for two of the designated FMUs. The Board supervises a third FMU because it has a state member banking license.[11]

Multiregional Data Processing Servicers

MDPS firms process mission-critical applications for a large number of financial institutions regulated by more than one agency or provide services in multiple locations throughout the country. Under the Bank Service Company Act of 1962,[12] the Board, together with the Office of the Comptroller of the Currency and the Federal Deposit Insurance Corporation (collectively, the federal banking agencies), has the authority to examine bank service companies performing key services to the same extent as if the bank performed the services itself on its own premises. These key services include facilitating payment and financial transactions, such as check and deposit processing; computing and posting interest and other credits and charges; or preparing and

9. The Board has not delegated its supervisory authority granted under title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act to the Reserve Banks.

10. Federal Reserve Banks perform supervisory activities for the financial institutions located within their respective Districts.

11. FMUs supervised by the Board are subject to risk management standards set out in Regulation HH and the Board's payment system risk policy. The risk management standards set out in both Regulation HH and the payment system risk policy are based on the *Principles for Financial Market Infrastructures* (PFMI). The PFMI, published by the Committee on Payment and Settlement Systems (now the Committee on Payments and Market Infrastructures) and the Technical Committee of the International Organization of Securities Commissions in April 2012, is widely recognized as the most relevant set of international risk management standards for payment, clearing, and settlement systems.

12. Bank Service Company Act of 1962, Pub. L. No. 87-856, 12 U.S.C. §§ 1861-67.

mailing checks, statements, and notices.[13] MDPS firms are the largest TSPs that have been selected for special monitoring and interagency supervision by the federal banking agencies. According to the FFIEC's *Supervision of Technology Service Providers* handbook, a financial institution's use of a TSP to provide products and services does not diminish the responsibility of the supervised institution to ensure that the service provider conducts the activities in a safe and sound manner and in compliance with applicable laws and regulations, just as if the institution were to perform the activities in house.

The Board's Current and Future Cybersecurity Oversight Approach

Board and System personnel currently perform a number of examination and nonexamination activities to assess and monitor cybersecurity risks at the financial institutions the Board oversees. As a part of examinations, examiners evaluate cybersecurity risks as a component of operational risk using the FFIEC IT Handbook. The IT Handbook provides guidance to examiners on how to assess the level of security risks 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. Examiners also conduct continuous monitoring activities to obtain updates on the supervised entities.[14]

To supplement these activities, examiners may conduct targeted examinations addressing specific business lines or systems within a financial institution. Further, examiners often perform horizontal reviews, which focus on one specific cybersecurity or information security topic across several financial institutions in order to identify portfolio-specific trends and recommendations.

Given the growth and complexity of cybersecurity threats in today's environment, the Division of Supervision and Regulation (S&R) recognized the need to enhance its existing frameworks and supervisory programs to assess the cybersecurity risks that exist to the largest and systemically important financial institutions. As a result, in 2015, S&R launched a multiyear program, known as the Cybersecurity Program Group (CPG), to improve and further develop the System's cybersecurity oversight program. This initiative was established (1) to issue cybersecurity risk policy and set expectations for financial institutions, (2) to develop examiner supervisory programs, (3) to build a cybersecurity surveillance and risk analysis infrastructure, (4) to increase cybersecurity training and assign examiners to institutions with the most risk, and (5) to implement robust continuous monitoring of cybersecurity risk-management program effectiveness at financial institutions.

According to S&R officials, the CPG is designed to build a cybersecurity program to establish, maintain, and communicate a theme-based set of expectations, leveraging policies, processes, and practices to reduce cybersecurity risk. The CPG includes six workstreams to accomplish these goals. The first workstream involves developing and maintaining an Advanced Framework that builds on past and ongoing work to assess the state of cybersecurity maturity for individual institutions and service providers, as well as the financial sector as a whole. In conjunction with

13. The Board considers MDPS firms to be bank service companies as defined by 12 U.S.C. § 1861(b)(2).

14. *Continuous monitoring activities* are nonexamination activities primarily designed to develop and maintain an understanding of the organization, its risk profile, and associated policies and practices.

the development of the Advanced Framework, S&R has also issued an advance notice of proposed rulemaking with the other federal banking agencies to solicit comments on a set of cybersecurity risk management and resilience standards that would apply to large and interconnected entities under their supervision, including third parties.[15] Based on the Advanced Framework, the CPG developed a Risk Analysis workstream to enable regulators to identify, evaluate, monitor, and measure current, emerging, and systemic cybersecurity risks and trends. To operationalize the Advanced Framework, the CPG created two workstreams to focus on examination methodology as well as training and resource coordination to enhance the approach, skills, and resources of cybersecurity examination teams. The CPG also developed a workstream for continuous monitoring to establish and monitor key risk and performance indicators at supervised entities. Finally, the CPG developed a workstream addressing intelligence and incident management to assess cybersecurity threats and trends, collect firm-specific information, as well as develop incident management protocols and coordinate cybersecurity exercises.

Scope and Methodology

The scope of our evaluation included the following areas:

- the governance of the Board's cybersecurity oversight program
- the project management of the Board's future-state CPG initiative
- the examination work performed for two of the Board's supervision portfolios: FMUs and MDPS firms

We selected this scope after conducting an extensive survey phase in which we researched relevant cybersecurity criteria used to conduct examinations, met with a number of Board and System personnel regarding the plans and progress of the CPG initiative, and interviewed stakeholders involved in the oversight of each Board supervision portfolio about their respective cybersecurity risks and oversight processes.

To achieve our objective, we focused our review of 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. Specifically, we reviewed a sample of completed examinations that were conducted within these two portfolios during 2014. We selected a judgmental sample of two Federal Reserve Banks to visit—the Federal Reserve Bank of New York (FRB New York) and the Federal Reserve Bank of Atlanta (FRB Atlanta) —that reflect the geographic dispersion of examination activities led by the Federal Reserve in 2014 within these two portfolios. For our individual Reserve Bank selections, we used the following criteria:

- We selected FRB New York because it supervises all the FMUs designated for primary oversight by the Federal Reserve and conducted 25 percent of the MDPS examinations led by the Federal Reserve in 2014.

- We selected FRB Atlanta because it also conducted 25 percent of the MDPS examinations led by the Federal Reserve in 2014, including a review of the largest firm in the portfolio.

15. More information about the advance notice of proposed rulemaking is available at https://www.federalreserve.gov/newsevents/press/bcreg/20161019a.htm.

We chose a judgmental sample of two of the three FMUs supervised by FRB New York, as well as four of the eight MDPS examinations led by the Federal Reserve in 2014 at FRB New York and FRB Atlanta. To review these examinations, we obtained access to the supervision plans and workpapers, assessed the work performed against relevant FFIEC and National Institute of Standards and Technology guidance, and conducted onsite interviews with supervisory personnel for each respective examination. Further, we met with Board and System officials responsible for governance and oversight of these supervisory activities.

With regard to S&R's efforts to enhance its cybersecurity oversight program, we evaluated the six workstreams of the CPG initiative to assess its plans to better identify, monitor, and measure cybersecurity risks to financial institutions. We also conducted interviews with Board and System personnel charged with implementing aspects of the CPG to evaluate the governance and project management practices of the project.

We conducted our fieldwork from May 2016 to October 2016. We performed our evaluation in accordance with the *Quality Standards for Inspection and Evaluation* issued in January 2012 by the Council of the Inspectors General on Integrity and Efficiency.

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

The Bank Service Company Act provides specific guidance to regulators, including the Board, to examine bank service companies that perform key services as if the services they provide are performed by the financial institution. We found that the Board (1) is not enforcing the requirement for financial institutions to report third-party relationships within 30 days, and therefore may not be fully aware of the total population of these firms; (2) has not created a specific portfolio in its governance structure to manage the unique risks associated with these firms; (3) has not provided supervisory guidance to examiners regarding third-party services; and (4) does not provide examiners with information about cybersecurity threats that could potentially affect MDPS firms. We generally attribute the current scope of the Board's activities regarding MDPS oversight to significant increases in the use of technology and bank service companies at financial institutions since the enactment of the Bank Service Company Act over 50 years ago. In addition, other priorities and supervisory portfolios have received greater attention within the System in recent years. Without a clear picture of the population of MDPS firms, an adequate oversight and governance structure, and supervisory guidance, Board and System personnel may not be effectively evaluating the cybersecurity risks associated with these firms.

The Bank Service Company Act 30-Day Requirement Is Not Being Enforced

As noted above, the Bank Service Company Act authorizes the Board to examine bank service companies that perform key services to the same extent as if the bank performed the services on its own premises. The Bank Service Company Act also requires that financial institutions notify their primary regulator of the existence of a vendor service relationship within 30 days of entering into a contract or a vendor performing a service, whichever occurs first.[16] However, the Board is currently not enforcing this 30-day requirement.

Since the Bank Service Company Act became law in 1962, the industry's reliance on third-party service providers has increased significantly. As a result, more clarity is needed regarding what constitutes a "service relationship" under the Bank Service Company Act. For example, the emergence of newer financial tools, such as digital payment systems, has made it difficult to discern what constitutes a "product" versus a "service," blurring the line as to whether the Board has oversight responsibilities. Further, a System official indicated that because financial institutions today have so many third-party service relationships, it is not realistic to enforce the reporting of a new relationship within 30 days. For example, this official noted that some of the largest institutions under the Board's supervision have approximately 10,000 to 25,000 service relationships. In these cases, the Board requests that each financial institution submit its 2,000 most critical vendor relationships.

Given the increased reliance on TSPs, as well as the need to clarify what constitutes a service, S&R may not be aware of all service relationships for the financial institutions it supervises. As a

16. 12 U.S.C. § 1867(c)(2).

result, the universe of TSPs and MDPS firms may not be fully known, increasing the likelihood of critical vendor cybersecurity risks going undetected during interagency supervisory efforts.

The Governance and Oversight Structure for MDPS Firms Does Not Address the Risk Profile of These Firms

S&R has established oversight and governance structures for various supervisory portfolios, such as Large Institution Supervision Coordinating Committee (LISCC)[17] firms, large domestic and foreign banking organizations,[18] and community banks.[19] The portfolio approach to supervision seeks to tailor the relative supervisory burdens for the institutions that make up those portfolios based on business models and risk associated with specific business activities. For example, as of the third quarter of fiscal year 2016, the LISCC portfolio contained 14 firms, including some of the largest bank holding companies in the nation.

According to the FFIEC, MDPS firms could pose a significant risk to the banking system if they experience operational or financial failures or disruptions, given the large number of financial institutions they serve, including banks, savings associations, and credit unions. However, our evaluation noted that the Board lacks 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, the Federal Deposit Insurance Corporation, and the Office of the Comptroller of the Currency. The federal banking agencies have identified 15 firms with the MDPS designation, with the largest organization servicing more than 11,000 clients and processing billions of transactions annually.

In the aftermath of the 2007 to 2009 financial crisis and the enactment of the Dodd-Frank Act, the Board focused significant attention on establishing a supervisory infrastructure for certain institutions, such as LISCC firms, due to their size, complexity, and importance in the financial sector. Further, because oversight of MDPS firms is shared among several federal regulators, the Board may have also prioritized establishing oversight structures for large, complex financial institutions because of its clear authority to supervise these entities. As we noted above, the System may not be fully aware of the universe of TSPs and MDPS firms, given its lack of enforcement of the 30-day reporting requirement in the Bank Service Company Act. Accordingly, the significance of this portfolio may not be fully appreciated, and while the use and size of these firms have grown tremendously over the past several years, the Board's oversight approach toward these firms has remained relatively static. The absence of a formal oversight structure for this portfolio may hinder the Board's efforts to effectively supervise these firms and mitigate cybersecurity risks.

17. The LISCC portfolio includes the largest and most complex domestic bank holding companies and foreign banking organizations that pose an elevated risk to U.S. financial stability, as well as other nonbank financial institutions designated as systemically important by FSOC.

18. Large banking organizations include domestic bank and savings and loan holding companies with consolidated assets of $50 billion or more and U.S. bank holding companies with total assets of $50 billion or more that are owned by foreign banking organizations and that are not included in the LISCC portfolio.

19. Community banks include domestic banks and savings and loan holding companies with consolidated assets up to $10 billion.

Examiners Lack Current Guidance From the Board on Overseeing MDPS Firms

The Bank Service Company Act authorizes the Board to "issue such regulations and orders as may be necessary to enable [it] to administer and implement the act."[20] S&R officials have indicated that the definition of what constitutes a service under the Bank Service Company Act is not clear in today's complex financial and IT environment. Since the enactment of the Bank Service Company Act in 1962, the services provided throughout the financial industry have evolved considerably as technology has advanced. The largest MDPS firms provide various services to financial institutions, including electronic funds transfer, automated clearing, credit card transactions, electronic banking, and other core banking services. In 1962, many of these services did not exist or were performed in house. An example of this evolution of technology services being outsourced throughout the financial sector is the use of cloud computing.[21] Use of a cloud provider may be considered a service for some financial institutions, depending on the nature of the arrangement made with the TSP. However, it is currently open to interpretation whether regulators have oversight authority for such services when they are outsourced by supervised financial institutions.

Examiners do not have current guidance from the Board on how to interpret the Bank Service Company Act in today's environment. This lack of guidance 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.

The Cybersecurity Program Group's Intelligence and Incident Management Workstream Is Not Aware of the Technologies Used by MDPS Firms

The CPG's Intelligence and Incident Management workstream developed a Cybersecurity Analytics Support Team (CAST) after a 2012 denial-of-service attack on a number of financial institutions. As a result of the attack, many supervision staff across the System felt that a greater awareness of the cybersecurity threat landscape was needed. CAST 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, we found that CAST is not fully aware of the technologies used by MDPS firms.

This lack of awareness could hinder the Board's ability to alert supervisory teams about specific cybersecurity intelligence and information. An example of this issue occurred in December 2015, when CAST became aware of intelligence involving a vulnerability in a specific network technology. The CAST alert for this incident noted that the technology is widely used throughout the financial sector and this risk may be concentrated in large, complex institutions; FMUs; and

20. 12 U.S.C. § 1867(d).

21. Cloud computing is a model for enabling convenient, on-demand network access to a shared pool of configurable computing resources (e.g., networks, servers, storage, applications, and services) that can be rapidly provisioned and released with minimal management effort or service provider interaction.

TSPs. Personnel involved in the CPG workstream informed the relevant examiners responsible for overseeing institutions reliant on this specific technology. However, there was no knowledge of which MDPS firms used the organization's technology, likely as a result of the limited guidance and governance structures in place for the MDPS portfolio. Consequently, examination teams for some firms affected by this vulnerability may not have been aware of this cyber-event and its effect on supervised entities.

As noted above, the Board has the authority to examine TSPs under the Bank Service Company Act. With this authority, the functionality offered by CAST could provide tremendous insight and value for the examination teams overseeing MDPS firms. Given the size and importance of the MDPS firms to the financial system, integration of MDPS-related data into the work performed by CAST could yield critical cybersecurity risk-based information for examination teams to consider during supervisory activities.

Recommendations

We recommend that the Director of S&R

1. 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.

2. 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.

3. 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 the expectations for supervising MDPS firms and TSPs.

4. Establish a process to document the IT systems being used at the MDPS firms and TSPs, and ensure that CAST is aware of this information so it can provide relevant cybersecurity alerts to supervisory teams.

Management's Response

In its response, S&R agrees with these recommendations and notes that the Federal Reserve System is currently working on a high-priority initiative (HPI) to develop and implement an integrated, nationally coordinated program for IT supervision that includes enhancing the oversight of these firms. As part of this initiative, S&R will work with other federal banking regulators to develop 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, develop a process for collecting this information, and periodically refresh the list of significant service providers. Further, S&R will work with other federal banking regulators and CAST to establish a process that identifies the technologies used by MDPS firms.

OIG Comment

In our opinion, the actions described by S&R are responsive to our recommendations. We plan to follow up on the division's actions to ensure that these recommendations are fully addressed.

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

S&R's strategic plan emphasizes the importance of programs to attract, retain, and maintain a highly qualified workforce to minimize the loss of institutional knowledge and to ensure successful leadership transitions. This specific priority is paramount for cybersecurity experts. Although the CPG has developed a workstream that focuses on the future state of cybersecurity training and resource coordination, we found that S&R has not yet addressed recruitment and retention planning, succession planning, resource tracking, and single-person dependencies for cybersecurity personnel. A key reason for these issues is the geographic dispersion of cybersecurity resources throughout the System, as well as the agency's focus on other competing initiatives and priorities. We believe that human capital and resource planning will be critical to the effectiveness of S&R's cybersecurity oversight program.

The Board Has Not Addressed Recruitment, Retention, and Succession Planning as a Part of the Cybersecurity Program Group's Planned Initiatives

Strategic human capital management has been a pervasive challenge for the federal government for the past several years. Since 2001, the U.S. Government Accountability Office has often identified strategic human capital management as a high-risk area affecting the government's ability to serve the American people. One area in which this challenge has been especially prevalent is cybersecurity. As the persistence and sophistication of cybersecurity threats continue to increase, so does the need for a workforce with the necessary skills, knowledge, and abilities to address complex and evolving cybersecurity challenges.

The Board recognized the importance of attracting and maintaining a highly qualified workforce in its *2016–2019 Strategic Plan*, identifying the shift in workforce demographics, the enhancement of talent management programs, and the use of human resources best practices as critical components to the execution of the agency's mission in an ever-changing environment. In alignment with the Board's strategic plan, S&R has also identified the importance of a resource management and allocation strategy to support the current and future needs of the supervision workforce through the acquisition, development, and retention of critical skills. A key success factor for this strategic goal is to develop programs focused on the specialty skills needed for critical System initiatives and high-priority work, such as the cybersecurity oversight approach being developed by the CPG.

The CPG's program structure consists of multiple components, including a workstream dedicated to enhancing the cybersecurity skills of examination teams and establishing mechanisms to share resources across the System more effectively. We found, however, that S&R has not yet addressed the recruitment, retention, and succession planning of cybersecurity resources. Further, we identified several key-person dependencies that exist within S&R's cybersecurity examination program that may present a risk to the viability and continuity of the function. These dependencies are a result of a shortage in cybersecurity talent, coupled with the geographic dispersion of cybersecurity personnel already employed throughout the System. Due to the

System's reliance on a nationwide pool of resources with cybersecurity skills, there is no central body responsible for the recruitment, retention, and succession planning of these individuals. Addressing and planning for these human capital management challenges may assist the Board and the System in attracting and retaining a highly qualified, diverse, and agile cybersecurity workforce while minimizing the risk of potential disruption or loss of institutional knowledge in critical cybersecurity oversight functions.

Resources Dedicated to Cybersecurity Oversight–Related Activities Are Not Formally Tracked

While the planning and allocation of resources are vital to aligning the workforce to meet strategic needs, the implementation of those plans is equally important. The S&R strategic plan for 2014–2018 notes that a key success factor for the division's goal of developing and implementing a resource management and allocation strategy is the use of a repeatable process to identify and understand the number, type, and location of resources and skill sets available to execute critical System initiatives, including cybersecurity. However, at the time of our review, we found that S&R was not using the Resource Optimization Activity Manager tool to track the resources allocated specifically to cybersecurity-related activities. Instead, cybersecurity resources were tracked under general examination activities or operational risk.

A key reason for this lack of specific tracking is the recent emergence of cybersecurity risks and threats as a significant component of the Board's oversight function. As the CPG continues its implementation, the number, type, and location of cybersecurity oversight–related activities will increase. By implementing a process to track the resources specifically allocated to cybersecurity-related activities, S&R officials will have more detailed and accurate information on the efficiency and effectiveness of cybersecurity resource allocations and management plans.

Management Actions Taken

Our fieldwork ended in October 2016, and our review included data as of that month. During the reporting phase of our evaluation, we learned that the CPG has begun to take steps to address the recruitment and retention of cybersecurity resources. Specifically, the Board has developed a framework to enhance its recruitment efforts for personnel with cybersecurity skills. Further, we also learned that the Board is exploring ways to enhance the capabilities of the Resource Optimization Activity Manager tool.

Recommendations

We recommend that the Director of S&R

5. Develop detailed recruitment, retention, and succession plans to ensure an agile, diverse, and highly qualified cybersecurity workforce.

6. 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.

7. Ensure that effective and repeatable processes are implemented to track cybersecurity resources in alignment with the Board's and the supervision function's strategic plans.

Management's Response

In its response, S&R agrees with these recommendations and notes that the division has initiatives underway to better manage the human capital associated with cybersecurity resources. A national recruitment program for new cybersecurity examiner positions, which will include national marketing, candidate screening, and interview processes, was approved as a part of the 2017 budget. S&R states that this centralized process for recruitment, retention, and succession planning should mitigate risks associated with resource dependencies. The division also requested a critical-needs exception to fill open cybersecurity examiner and analyst positions after the federal government announced a hiring freeze in late January 2017. Further, efforts are underway to implement a tracking standard for cybersecurity resources across supervisory portfolios using the Resource Optimization Activity Manager tool.

OIG Comment

In our opinion, the actions described by S&R are responsive to our recommendations. We plan to follow up on the division's actions to ensure that these recommendations are fully addressed.

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

In 2014, S&R issued Advisory Letter (AD Letter) 14-10, *Enhancing Supervisory Risk Identification, Monitoring, and Mitigation*. The letter highlights that risk identification and monitoring in the System involves many parties, including system management groups, the Surveillance function, Reserve Banks' risk structures, System risk coordinators, affinity groups, and others. The letter further recognizes that this approach does not fully synthesize information from such sources. We found that cybersecurity and IT risks are currently assessed within individual supervisory oversight portfolios and are highlighted in a semiannual report for select stakeholders. In addition, cybersecurity issues identified during examinations have been communicated to these stakeholders on an ad hoc basis; however, this information is not regularly communicated to other relevant stakeholders, including System supervision personnel responsible for cybersecurity oversight. We attribute this issue to the lack of a formalized communications plan to share cybersecurity risks with these parties. As noted above, cybersecurity has emerged as one of the top risks to the financial sector over the past several years. If Board and System officials do not receive timely information on critical IT and cybersecurity issues across portfolios, their ability to make informed supervision and policy decisions could be negatively affected. In addition, a lack of awareness of the range of risk identification efforts across the System can lead to unnecessary duplication of efforts or gaps in supervisory coverage.

No Formalized Communications Plan Exists to Regularly Communicate Critical IT and Cybersecurity Issues to the System

S&R relies on multiple sources to identify and monitor risk issues affecting the System. These entities include system management groups that oversee the Board's portfolios, the Surveillance function, Reserve Banks' risk structures, and System risk coordinators. Additionally, S&R has several leadership committees responsible for providing guidance on various supervision-related matters. In AD Letter 14-10, the Board identified that its process for assessing the output from these sources could be improved. As a result of this guidance, S&R implemented a new framework that aimed to (1) create an infrastructure for the collection and sharing of risk information, (2) develop a System risk report that synthesizes risk information, and (3) implement a System Risk Council to analyze risk information and develop recommendations. According to AD Letter 14-10, the Risk Council will issue its recommendations to the S&R policy function.

The Risk Council produces a semiannual report that highlights various risks facing the banking system, including risks related to cybersecurity. Additionally, in 2016, two ad hoc surveillance reports were produced and presented to the Risk Council, highlighting specific cybersecurity issues[22] identified during previous examinations. Although the members of the Risk Council are receiving these reports, we found that there is no formalized plan to regularly

22. These reports highlighted cybersecurity-related matters requiring attention and matters requiring immediate attention identified during previous examinations.

communicate these results to other relevant personnel, including System supervision personnel responsible for cybersecurity oversight. Providing these reports to personnel responsible for cybersecurity oversight on a need-to-know basis could be a useful supplement to the CAST intelligence reporting and could help to inform supervisory approaches and decisions.

Management Actions Taken

In 2016, S&R published an HPI to develop a cybersecurity strategy and evaluate potential changes to its cybersecurity supervisory approach. The project intended to achieve this HPI is the CPG initiative, which has several deliverables, including a cybersecurity risk-assessment methodology, a risk profile and maturity model, as well as a risk rating methodology and identification of key cybersecurity supervisory themes to better allow Board and System management to form an integrated, holistic view of material cyber and IT risks across all portfolios in a sustained manner. This HPI has been renewed by S&R for 2017, and progress continues on the implementation of the CPG as the future state of S&R's cybersecurity oversight program. Additionally, S&R developed a new HPI for 2017 to assess the current state of IT supervision for financial institutions and service providers, as well as the implications for safety and soundness across all portfolios. With the issuance of the advance notice of proposed rulemaking, along with the ongoing implementation of the CPG, we will continue to assess the changes made to S&R's cybersecurity supervision function as they relate to the communication and aggregation of cybersecurity risk across portfolios as a part of our future work.

Recommendation

We recommend that the Director of S&R

8. 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.

Management's Response

In its response, S&R agrees with this recommendation and notes that efforts to address cybersecurity and IT risks would benefit from enhanced visibility and focus. 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, is fully informed of all cybersecurity risks across portfolios. The Risk Council is also developing a plan to improve the communication of key risk issues to System stakeholders. Further, as a part of the cybersecurity HPI, S&R will be working with CAST as it conducts daily monitoring of the financial sector and reports on cybersecurity threats from a supervisory perspective.

OIG Comment

In our opinion, the actions described by S&R are responsive to our recommendation. We plan to follow up on the division's actions to ensure that this recommendation is fully addressed.

Appendix A
Management's Response

BOARD OF GOVERNORS
OF THE
FEDERAL RESERVE SYSTEM
WASHINGTON, D.C. 20551

DIVISION OF SUPERVISION
AND REGULATION

April 10, 2017

Mr. Mark Bialek
Inspector General
Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue, NW
Washington, DC 20551

Dear Mark:

Thank you for the opportunity to comment on the draft report, *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third Party Service Provider Oversight, Resource Management, and Information Sharing*. We appreciate the effort that the Office of the Inspector General (OIG) has put into this evaluation and the recommendations it has provided for improving our cybersecurity supervision.

We agree with the overarching goal of the evaluation to enhance the Federal Reserve's approach to cybersecurity supervision as it continues to implement its multi-year, future-state cybersecurity oversight program. The Federal Reserve System is currently taking steps to support that goal, including implementation of two high-priority initiatives (HPIs), one to implement the cybersecurity strategy and change in supervisory approaches, and the second to assess the current state of IT supervision.

The report provides eight recommendations for enhancing the Federal Reserve's approach to cybersecurity supervision. Our team agrees with all of the recommendations and is in the process of implementing many of them. We have grouped our responses across three primary themes: (1) enhancement of the oversight of multiregional data processing servicers; (2) better management of human capital associated with its cybersecurity resources; and (3) benefits to cybersecurity and IT risk through enhanced visibility and focus. While our responses are organized by theme, we recognize the need to address each recommendation individually.

1. Enhancement of the Oversight of Multiregional Data Processing Servicers (Recommendations 1, 2, 3, and 4)

   We agree with the recommended enhancements to the oversight of multiregional data processing servicers. The Federal Reserve System is currently working on a HPI to develop and implement an integrated, nationally coordinated program for IT supervision that includes enhancing the oversight of these firms. This initiative includes evaluating enhancement options and implementing an appropriate governance structure. The Federal Reserve will work with the other federal banking regulators to develop additional guidance on the identification of service providers and supervisory expectations. Part of this initiative will be to notify financial institutions of the requirement for reporting new

service provider relationships, developing a process for collecting this information, and periodically refreshing the list of significant service providers (SSPs). The Federal Reserve will also work with the other federal banking regulators and the Cybersecurity Analytics Support Team (CAST) to establish a process that identifies technologies used at multiregional data processing services.

2. Better Management of Human Capital Associated with its Cybersecurity Resources (Recommendations 5, 6, and 7)

   We agree with the recommendations and have initiatives underway to better manage human capital associated with cybersecurity resources. In the 4th quarter of 2016, the Federal Reserve implemented a national recruitment program for the new cyber security examiner positions that were approved with the Federal Reserve System's 2017 budget. The program includes a national marketing, candidate screening, and interview process. National recruitment continued until the Federal Government hiring freeze was announced in late January 2017. We are currently requesting a critical need exception to fill open cyber risk examiner and analyst positions.

   The centralized approaches for the recruitment, retention, and succession planning will assist in mitigating risks associated with resource dependencies. Additionally, efforts are underway to develop and implement a System standard for tracking the allocation of cyber examination resources across the supervision portfolios through utilization of the System's Resource Optimization Activity Manager (ROAM) tool.

3. Benefits to Cybersecurity and IT risk through Enhanced Visibility and Focus (Recommendation 8)

   We agree with the recommendation that cyber and IT risks would benefit from enhanced visibility and focus. In 2017, the Risk Council is taking steps for cyber risk, a component of operational risk, to be presented as a standalone topic at a minimum once, if not twice, a year to ensure the Council is fully informed of all cyber risks across all portfolios and all Federal Reserve-supervised SSPs. The Risk Council is also putting together a plan to improve communication of key risk issues to System stakeholders as a part of its 2017 goals.

   Through the work of the cybersecurity HPI, there will also be a focus on identifying and reporting emerging threats and key cyber risk themes across all portfolios. We will be working with CAST as they conduct daily monitoring of the financial sector and reporting on cyber threats from a supervisory perspective. In addition to the HPI to assess the current state of IT supervision, we believe these initiatives will improve the communication and aggregation of cyber risk across the portfolio.

Thank you for the opportunity to provide comments on this report. We are committed to addressing the recommendations and taking the necessary steps to enhance the Federal Reserve's cybersecurity supervisory program.

Regards,

Maryann F. Hunter
Acting Director

OFFICE OF INSPECTOR GENERAL

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

HOTLINE

1-800-827-3340

OIGHotline@frb.gov

Report Fraud, Waste, and Abuse

Those suspecting possible wrongdoing may contact the OIG Hotline by mail, e-mail, fax, or telephone.

Office of Inspector General, c/o Board of Governors of the Federal Reserve System
20th Street and Constitution Avenue NW, Mail Stop K-300, Washington, DC 20551
Attention: OIG Hotline

Fax: 202-973-5044

Questions about what to report?

Visit the OIG website at www.federalreserve.gov/oig
or
www.consumerfinance.gov/oig