OFFICE OF INSPECTOR GENERAL

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

September 27, 2017

MEMORANDUM

TO: Board of Governors

FROM: Mark Bialek
Inspector General

SUBJECT: 2017 List of Major Management Challenges for the Board

We are pleased to provide you with the Office of Inspector General's (OIG) 2017 list of major management challenges facing the Board of Governors of the Federal Reserve System (Board). These challenges represent what we believe to be the areas that, if not addressed, are most likely to hamper the Board's accomplishment of its strategic objectives.

We identified the Board's major management challenges by reviewing our audit and evaluation work, reports issued by the U.S. Government Accountability Office, and Board documents. We note that the challenges we have identified relate to strategic pillars, objectives, or initiatives contained in the Board's *Strategic Plan 2016–19*. The following table lists the five management challenges, in order of significance.

Each challenge is listed below.

Enhancing Governance, Including Using an Enterprise Approach to Carry Out Agencywide Functions

An effective governance system provides leadership, direction, and accountability in fulfilling an organization's mission and provides stewardship of public resources while establishing clear lines of responsibility for results. The Board has a complex governance system that presents challenges to using an enterprise approach to manage agencywide administrative functions and activities, such as human capital management, information technology (IT) services, physical infrastructure, and internal controls and risk management. The Board's decentralized structure and the lack of a single authority for these activities has resulted in redundancies and potentially higher costs in certain areas.

Human Capital Management

The Board's success in achieving its mission is contingent on attracting, retaining, and developing a qualified, diverse, and agile workforce. But evolving workforce expectations and a highly competitive hiring environment for those with the skills required by the Board create challenges in developing such a workforce. Moreover, current and long-term budget pressures and an expected rise in the number of Board employees eligible for retirement may contribute to gaps in leadership and institutional knowledge, as well as complicate existing human capital challenges. Improved human capital management will be required to mitigate these challenges and meet future workforce needs.

One key human capital initiative is workforce planning, which can help the Board strengthen its human capital management by identifying critical skills and competencies. Workforce planning encompasses a range of activities, such as identifying future human capital needs, leveraging existing talent to meet those future needs, and building a diverse pipeline of potential successors for mission-critical positions. Since 2016, when we reported that the Board faced challenges in developing and implementing a Boardwide strategic workforce-planning framework, the Board has (1) begun to adopt a more strategic approach to workforce planning that assesses how the placement of vacant positions and the requisite skill sets can best meet the Board's workforce needs and (2) improved its process to attract diverse, highly qualified employees. Specifically, the Board has identified workforce as a priority in its 2016–2019 strategic plan, hired human capital staff members with expertise in workforce planning, begun to develop a workforce planning pilot program, and finalized its diversity and inclusion strategic plan.

The Board plans to continue its efforts to implement a more strategic approach to workforce planning and improve its human capital management, including enhancing performance management; succession planning; and the recruitment of diverse, highly qualified staff. The Board has also taken steps to enhance and promote diversity and inclusion by implementing corrective actions that addressed all the recommendations in our March 31, 2015, report, *The Board Can Enhance Its Diversity and Inclusion Efforts*. The challenge remains for the Board to implement enterprisewide human capital improvements, including workforce planning and diversity and inclusion initiatives, in a strategic and effective manner.

Governance over the human capital function may also create challenges. The Board's diversity and inclusion program is not managed by the same division that manages the human capital program; these programs need to be well coordinated. The Chief Human Capital Officer (CHCO), an officer in the Management Division, is responsible for overseeing the Board's operations and resources related to personnel management; however, the CHCO is not authorized to formulate, approve, or implement policies for enterprisewide personnel management. That authority lies with the Director of the Management Division, who is two levels above the CHCO. Because of the limitations on the position's authority and organizational placement, the CHCO faces challenges overseeing the implementation of enterprisewide human capital initiatives.

IT Services

Although the Division of Information Technology provides agencywide IT services and manages the Board's information security program, some divisions also have their own IT sections, which can result in operational inconsistencies as well as higher costs due to the duplication of efforts. In addition to cost inefficiencies, the Board's decentralized IT structure contributes to challenges in implementing an effective information security continuous monitoring and risk management program, as further detailed in the management challenge Ensuring an Effective Information Security Program below. In our *2016 Audit of the Board's Information Security Program*, we found that the Board's Information Security Officer does not have an effective level of visibility into the people, processes, and technologies that are employed by Board divisions that maintain their own IT sections. The decentralized IT structure has also limited the ability of the Board to effectively deploy enterprisewide solutions to centralize and automate information security continuous monitoring and risk management processes.

Physical Infrastructure

Ensuring that the Board has the physical infrastructure it needs to carry out its mission in a cost-effective manner presents significant risks and challenges, including those associated with contractor oversight, cost management, and disruptions to employees. The Board's challenges in these areas relate to a portfolio of activities, including renovating the William McChesney Martin, Jr., Building (Martin Building), renovating the New York Avenue facility, managing and building out leased space, and designing space for efficient use as workforce demographics change. In addition, the Board recently announced plans to explore the renovation of the Marriner S. Eccles Building (Eccles Building).

On the Martin Building project, which is one of the Board's largest contracting efforts, the Board is responsible for overseeing the firm conducting the design work, acquiring and managing a general construction contractor, and managing support vendors. The design work for the project resumed in 2013 after significant delays and scope changes, and current estimates are that the project will be completed in 2020. With regard to the other projects, the Board is building out leased space for three divisions that are relocating from other Board leased and owned space. In the New York Avenue facility, a floor of the building last updated in the 1990s is being redesigned with updated office layouts and new fixtures. These other projects are scheduled for

completion in late 2017 and the last quarter of 2018, respectively. The infrastructure projects in the Board's portfolio are interrelated, and any delays could have cascading effects on completion dates and costs.

In 2007, the Board began to supplement its owned space with leased space, and in 2012, the Board acquired additional leased space both to accommodate overall staff growth and to house staff displaced due to the Martin Building renovation and other infrastructure projects. As of June 2017, the Board maintained multiple leases in two separate facilities. Although when completed, these projects will provide Board employees with updated workspace, the Board's current staffing level requires the Board to house employees in leased space spread over multiple locations. While considering long-term space options, the Board noted that the current approach of maintaining multiple leases is costly and impedes employee engagement when compared with a consolidated-campus approach.

In response to challenges associated with these infrastructure projects, the Board monitors project schedules and milestones for capital projects in bimonthly reports to the Chief Operating Officer or quarterly reports to the Investment Review Board. Further, to ensure that the renovation of the Martin Building remains on schedule, the Board has regular meetings with its contractors to discuss project progress, resolve outstanding issues, monitor the schedule, and review other pertinent matters. In addition, the Board has developed space-planning strategies that cover short-, medium-, and long-term time frames. These strategies include options such as continuing to lease space in multiple locations in the short term and consolidating leased space into fewer locations in the long term. In developing these strategies, the Board is considering factors such as building location limitations, staffing levels, technological requirements, and the implications of telework.

Following a building condition assessment in 2017, the Board announced that an architectural and engineering design review will be conducted as part of an effort to explore the renovation of the 80-year-old Eccles Building. Renovation of the Eccles Building may pose challenges that are similar to those posed by the Martin Building project. The Board has stated that procurement efforts for the design of the possible Eccles Building renovation project will begin in 2017 and that Board divisions will have an opportunity to provide input on the design effort.

Internal Control and Risk Management

The Board's current governance system also contributes to the inconsistent implementation and monitoring of administrative internal controls. In a 2013 report, we identified the need for an agencywide policy and process for maintaining and monitoring internal controls. In 2016, the Office of Management and Budget released *OMB Circular No. A-123: Management's Responsibility for Enterprise Risk Management and Internal Control*. This circular instructs federal agencies to coordinate their internal control processes with their enterprise risk-management capability and strategic planning and review processes. The Board is not required to follow this circular and, to date, has made limited progress in establishing agencywide internal control processes or an enterprise risk-management system to manage the risks it faces as it works to achieve its strategic objectives or that arise from its activities and operations.

In its strategic plan, the Board identifies initiatives to improve its governance system, including (1) establishing governance that more effectively prioritizes resources within the constraints of the budget, (2) defining a governance plan for the Board's use of technology, and (3) implementing a data governance framework. Additionally, in January 2017 the Board hired a senior advisor with specialized experience to assess and develop its enterprise risk-management program.

Related OIG Reports

- *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016
- *The Board Can Enhance Its Diversity and Inclusion Efforts*, OIG Report 2015-MO-B-006, March 31, 2015.
- *The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control*, OIG Report 2013-AE-B-013, September 5, 2013

Other Related Information

- Board of Governors of the Federal Reserve System, *Strategic Plan 2016–19* (Strategic Pillar: Project Development and Resource Allocation, page 9; Strategic Pillar: Technology, page 11; and Strategic Pillar: Data, page 12)
- Board of Governors of the Federal Reserve System, *Diversity and Inclusion Strategic Plan 2016–19*
- Office of Management and Budget, *OMB Circular No. A-123: Management's Responsibility for Enterprise Risk Management and Internal Control*, Memorandum M-16-17, July 15, 2016

Enhancing Oversight of Cybersecurity at Supervised Financial Institutions

Over the past several years, as financial institutions have continued to adopt internet-based systems to conduct business, the number and sophistication of cyberthreats to the financial sector have increased dramatically. As a result, 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. Accordingly, financial institutions and regulators must prepare for potential significant cyberattacks.

The Board's supervisory program for financial institutions includes efforts to ensure that supervised financial institutions manage and mitigate risks and vulnerabilities associated with cyberattacks. As the number and sophistication of cyberthreats to and cyberattacks at financial institutions increase, the Board faces challenges in ensuring that supervisory approaches keep pace with evolving cyberthreats as well as concerns of the financial services sector. The Board also faces challenges in continually tailoring its supervisory approach for the various institutions it supervises. For example, the Board must enhance its oversight of firms that provide technology services to supervised entities. The Board can enhance its oversight by implementing an improved governance structure and providing additional guidance to examination teams on the supervisory expectations for such firms. In addition, the Board must improve the recruitment and retention, as well as succession planning, of cybersecurity resources to ensure an agile, diverse, and highly qualified cybersecurity workforce. The Board must also enhance its communication of critical IT and cybersecurity-related risks to relevant Board and Federal Reserve System supervision personnel.

The Board's Cybersecurity Program Group is a multiyear initiative to further develop the Federal Reserve System's cybersecurity oversight program. The Cybersecurity Program Group continues to enhance supervisory program components, such as training and resource coordination, risk analysis, incident management, and other work streams, to guide future IT examinations. We will continue to monitor the Board's progress to enhance its oversight of cybersecurity at financial institutions.

Related OIG Reports

- *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing,* OIG Report 2017-IT-B-009, April 17, 2017

Other Related Information

- U.S. Government Accountability Office, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information*, GAO-15-509, July 2, 2015

Ensuring an Effective Information Security Program

Cyberthreats can be targeted or untargeted attacks from criminals, hackers, disgruntled employees, and other organizational insiders, among others, and can be intentional or unintentional. Information security continues to be a key risk in the federal government, as demonstrated by recent incidents involving breaches of sensitive data and the sharp increase in information security incidents reported by federal agencies over the last several years. The Board faces challenges in enhancing its information security program in the areas of information security continuous monitoring, risk management, and oversight of third-party providers.

The Board is required by the Federal Information Security Modernization Act of 2014 to develop, document, and implement an information security program to protect its information systems and data. To address this requirement, the Board has developed and implemented a Boardwide information security continuous monitoring program. Although the program is generally consistent with federal requirements, our work has identified opportunities for the Board to ensure that its information security continuous monitoring program is effective through greater centralization and automation.

Similarly, the Board faces challenges in implementing a Boardwide risk management program to encompass Board divisions that independently manage their own IT infrastructure. As noted in our *2016 Audit of the Board's Information Security Program*, we found that Board divisions were not consistently implementing the organization's risk management processes related to security control assessments, security planning, and authorization. These weaknesses were the result of the Board's decentralized IT structure and inconsistent oversight of the Board's risk management program. This structure has resulted in the Board's Chief Information Officer not having an effective level of insight and authority over the IT functions performed across the Board. Lastly, although the Board uses an enterprise data-loss prevention solution and has developed a draft insider-threat plan for classified information, it has not determined the most efficient ways to manage the risk from insider threats for sensitive agency information that is maintained in its internal systems.

The Board relies on third-party providers, including the Federal Reserve Banks, to support its IT needs. The Reserve Banks provide IT solutions in support of certain delegated Board functions. The Board has strengthened its program to oversee third-party providers; however, the Board continues to face challenges in ensuring that the Reserve Banks' information security controls are implemented and maintained and monitored in accordance with Board requirements.

Consistent with the requirements of the *Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure*, the Board is in the process of aligning its information security program and related policies and procedures to the National Institute of Standards and Technology Cybersecurity Framework. This alignment will enable the Board to continue improving its information security program, including strengthening access controls and processes to ensure that third-party providers meet the requirements of the Federal Information Security Modernization Act of 2014.

Related OIG Reports

- *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016
- *2015 Audit of the Board's Information Security Program*, OIG Report 2015-IT-B-019, November 13, 2015

Other Related Information

- U.S. Government Accountability Office, *High-Risk Series*: *Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, "Ensuring the Security of Federal Information Systems and Cyber Critical Infrastructure and Protecting the Privacy of Personally Identifiable Information," GAO-17-317, February 15, 2017

Continuing to Strengthen the Regulatory and Supervisory Framework While Remaining Sufficiently Nimble to Address Potential Internal or External Developments

Promoting the safety, soundness, and stability of financial institutions and financial market infrastructures is a core activity supporting the Board's mission. The Board should continue to build on its progress in recent years to enhance its regulatory and supervisory framework while remaining sufficiently nimble to address potential developments that could influence the direction of its supervisory efforts. The Board's challenges include (1) responding to regulatory changes and organizational developments, (2) leveraging and enhancing the existing technology infrastructure that supports supervisory activities, (3) fostering a culture that encourages employees to share their views on supervision matters, and (4) maintaining effective relationships with other regulators.

The Board must be sufficiently nimble to respond to regulatory changes and organizational changes that could influence the strategic direction of its supervisory efforts. A congressional effort to reconsider some of the financial service regulatory policies and approaches resulting from the enactment of the Dodd-Frank Wall Street Reform and Consumer Protection Act is ongoing, and the Board will have to address any potential changes. In addition to the potential for legislative changes, the appointment of a new Vice Chair for Supervision will have an influence on the Board's supervision program. These developments, combined with resource constraints, will require a high degree of adaptability.

Data and information management continue to increase in importance and complexity, and the Board has acknowledged the need to be prepared to augment its technology infrastructure to support increased data needs. Further, the Board must continue to leverage and enhance its IT tools to effectively and efficiently conduct its supervision activities.

Given the complexity associated with assessing risks at many large financial institutions with nuanced business activities, the free flow of information between supervision employees and their leaders has proven to be crucial to the effectiveness of the Board's supervisory efforts. The Board should continue to foster a culture and take measures to encourage employees to share their views, including opposing views, so that decisionmakers reach informed conclusions and decisions about supervised entities.

To effectively execute its duties as the consolidated supervisor for bank, financial, and savings and loan holding companies, the Board must continue to cultivate and maintain strong cooperative relationships with the primary supervisors of holding company subsidiaries.

Effective collaboration with other regulators also helps the Board monitor and identify emerging and systemic risks. Continued efforts to coordinate with other federal supervisory agencies are crucial to the Board's effective execution of its supervisory responsibilities because this coordination can (1) reduce potential duplication of efforts or eliminate gaps in supervisory coverage and (2) help identify and monitor emerging risks.

The Board continues to take measures to enhance its oversight framework for banking organizations and will have to be sufficiently nimble to respond to changes that could influence the strategic direction of its supervisory efforts. The Board also continues to improve the usability of technological tools in support of its supervisory activities. In addition, the Board is implementing a high-priority initiative to encourage constructive dialog and rigorous debate among financial institution supervisory employees at all levels to improve decisionmaking across the Federal Reserve System. In furtherance of its supervisory efforts, the Board continues to coordinate with its counterparts to align strategic objectives and minimize duplicative efforts. We will continue to monitor the Board's progress to strengthen its supervisory and regulatory framework amid potential internal or external developments.

Related OIG Reports

- *The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool*, OIG Report 2017-SR-B-005, March 29, 2017

- *Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities*, OIG Report 2016-SR-B-014, November 14, 2016

- *The Board Should Enhance Its Supervisory Processes as a Result of Lessons Learned From the Federal Reserve's Supervision of JPMorgan Chase & Company's Chief Investment Office*, OIG Report 2014-SR-B-017, October 17, 2014

Other Related Information

- U.S. Government Accountability Office, *2016 Annual Report: Additional Opportunities to Reduce Fragmentation, Overlap, and Duplication and Achieve Other Financial Benefits*, GAO-16-375SP, April 13, 2016

Managing the Handling and Release of Sensitive Federal Open Market Committee and Board-Generated Information

Sensitive Federal Open Market Committee (FOMC) and Board-generated information has the potential to significantly influence financial market activity and affect public policies and private sector decisions. Accordingly, the Board has a responsibility to effectively manage the handling and release of such information. Although the Board has taken a number of steps to enhance its

controls in this area, events over the past several years indicate continuing challenges in managing the handling and release of sensitive FOMC and Board-generated information provided to news organizations under embargo and posted on the Board's public website.

Recent events indicate continuing challenges in this area. We have previously noted incidents of inadvertent and premature postings that occurred in 2015 and 2016. We are also aware of three similar events that occurred in 2017. Although these events did not significantly influence financial market activity, they highlight continued weaknesses.

The Board has taken steps to strengthen its controls surrounding the handling and release of sensitive FOMC and Board-generated information. These steps include the implementation of a data loss prevention program, which helps reduce the risk of employees inadvertently sending sensitive information via electronic media; improvements in the processes and controls in place to safeguard sensitive economic information provided to news organizations under embargo; and better controls over sensitive information prior to scheduled release on the Board's public website. Although these actions have helped to improve the Board's information control environment, recent events demonstrate that protecting potentially sensitive information from unauthorized or premature disclosure continues to be a challenge for the Board. The Board is continuing to implement process improvements associated with its handling and release of sensitive FOMC and Board-generated information.

Related OIG Reports

- *2016 Audit of the Board's Information Security Program*, OIG Report 2016-IT-B-013, November 10, 2016
- *The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations*, OIG Report 2016-MO-B-006, April 15, 2016
- *2015 Audit of the Board's Information Security Program*, OIG Report 2015-IT-B-019, November 13, 2015

Closing

We are monitoring the Board's efforts to address the management challenges highlighted in this document. Our monitoring work includes following up on open recommendations and conducting related audit and evaluation work. For additional information on our ongoing and planned work, please see our *Work Plan*.

We appreciate the cooperation that we received from the Board during this year's management challenges process. If you would like to discuss any of the challenges, please feel free to contact me.

cc: Donald V. Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Ricardo Aguilera, Chief Financial Officer and Director, Division of Financial Management
Mark Van Der Weide, General Counsel, Legal Division
Eric Belsky, Director, Division of Consumer and Community Affairs
Michell Clark, Director, Management Division
Matthew J. Eichner, Director, Division of Reserve Bank Operations and Payment Systems
Michael S. Gibson, Director, Division of Supervision and Regulation
Steven B. Kamin, Director, Division of International Finance
Thomas Laubach, Director, Division of Monetary Affairs
Andreas Lehnert, Director, Division of Financial Stability
Ann E. Misback, Secretary of the Board, Office of the Secretary
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Michelle A. Smith, Assistant to the Board, Chief of Staff, and Director, Office of Board Members
David Wilcox, Director, Division of Research and Statistics