OFFICE OF INSPECTOR GENERAL
BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM
CONSUMER FINANCIAL PROTECTION BUREAU

September 30, 2015

MEMORANDUM

TO: Board of Governors

FROM: Mark Bialek
Inspector General

SUBJECT: 2015 List of Major Management Challenges for the Board

We are pleased to provide you with the Office of Inspector General's 2015 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 used audit and evaluation work performed by our office, audits performed by the U.S. Government Accountability Office, and the Board's strategic planning documentation to identify these major management challenges. This year, we are adding a challenge, Enhancing Oversight of Cybersecurity at Supervised Financial Institutions, in recognition of the difficult challenges the Board faces in continuing to promote the safety and soundness of financial institutions in an environment in which cyberthreats are increasing and becoming more sophisticated. The table below lists the six management challenges we have identified, in order of significance.

Each challenge is detailed below.

Management Challenge 1: Enhancing Oversight of Cybersecurity at Supervised Financial Institutions (NEW)

In January 2015, the President stated that cyberthreats pose one of the most serious economic and national security challenges we face as a nation. Cyberattacks are a growing operational risk to the critical infrastructure of the United States, including its financial system. The threat of cyberattack is a constant presence in the government information technology (IT) environment, as exemplified earlier this year, when the U.S. Office of Personnel Management reported its detection of cybersecurity incidents affecting its systems and data. These incidents compromised the personal information of current and former federal employees, prospective federal employees, and contractors. There also have been many recent high-profile instances of cyberattacks on financial institutions as well as on other private- and public-sector entities.

Banks have responded to the increasing rate, frequency, and complexity of attacks by strengthening network and perimeter defenses, further protecting client and sensitive information, engineering tighter controls, and investing in tools and analytics to study system patterns and to spot anomalous activity. These institutions will continue to face challenges in defending against a constantly evolving cybersecurity landscape with new threats.

The Board's supervisory program for financial institutions is adding resources to bolster its efforts to ensure that supervised financial institutions manage and mitigate the potential risks and vulnerabilities associated with cyberattacks. As the use of technology continues to become more sophisticated, hiring and training sufficient numbers of staff with the expertise needed to conduct detailed examinations of information security systems presents a challenge.

As cyberthreats continue to evolve, the Board faces challenges in appropriately tailoring and keeping current its supervisory approach to the various types of institutions it supervises. Those institutions include community banking organizations, regional banking organizations, large banking organizations, and Large Institution Supervision Coordinating Committee portfolio firms,[1] as well as certain technology service provider companies and systemically important payment, clearing, and settlement companies that support these institutions. According to the U.S. Department of the Treasury, effective public-private coordination will be required to address the growing threat of cyberattacks against the nation's critical infrastructure. As such, effective interagency coordination among the federal financial regulators as well as between the Board and its supervised institutions is critical. As the governing body of the nation's central bank, the Board is expected to facilitate the smooth functioning of critical financial infrastructure, such as the payment system, as well as take a leadership role in developing and adapting expectations in this area to ensure that regulated institutions manage vulnerabilities.

1. Financial institutions are classified according to total asset size. Financial institutions with total assets of less than $10 billion are community banking organizations, institutions with total assets of $10 billion to $50 billion are regional banking organizations, and institutions with total assets greater than $50 billion are large banking organizations. The Large Institution Supervision Coordinating Committee portfolio includes large financial institutions that may pose risks to the financial system as a result of critical securities clearing, processing businesses, or other systemically important functions.

The Board faces challenges in adapting its overall supervisory approach to cybersecurity's evolving landscape. The Board requires the financial institutions it supervises to develop and maintain effective information security programs that are tailored to the complexity of each institution's operations. The Board also requires these institutions to develop and implement programs to respond to data breaches. As cyberthreats and attacks at financial institutions increase in number and sophistication, the Board faces challenges in tailoring and updating its supervisory approach appropriately, defining short- and long-term goals, and working with other financial regulators to provide support and guidance to its supervised institutions.

Agency Actions

The Board is coordinating across Federal Reserve lines of business and is managing and participating in several cybersecurity initiatives with both public and private organizations. To provide regulatory oversight to financial institutions, the Board has created a cyberprogram group to help prioritize cyberrisks that could interrupt commerce and financial institutions. This group is developing an assessment framework to conduct cybersecurity examinations, preparing to conduct training for supervised institutions, and prioritizing resources within the Board. The group also has developed policies and regularly updates its supervisory approach in response to the constantly changing cybersecurity landscape.

The Board has also worked with the other members of the Federal Financial Institutions Examination Council (FFIEC) to develop a new Cyber Resilience part for the Business and Continuity Planning section of the *FFIEC Information Technology Examination Handbook* and to develop and release an FFIEC Cyber Assessment Tool, which will give financial institutions a resource for conducting self-assessments of cyberpreparedness. The Board is also a member of the Financial and Banking Information Infrastructure Committee, which is charged with improving coordination and communication among financial regulators, enhancing the resiliency of the financial sector, and promoting public-private partnerships. Finally, according to the Director of the Division of Banking Supervision and Regulation, Large Institution Supervision Coordinating Committee supervisory teams are engaging with the most systemically important institutions regarding each firm's cybersecurity program and are assessing the current state of institutions' cyberpreparedness.

Management Challenge 2: Ensuring an Effective Information Security Program

Protecting information systems and the nation's cybercritical infrastructure remains a priority for federal agencies, as reported by the U.S. Government Accountability Office. Information security is a priority for the Board as it continues to implement existing and new federal requirements. New federal requirements include developing an enterprise-wide continuous monitoring program and an enterprise-wide risk management program. The Board must also persist in its efforts to ensure that information systems and services provided by third-party providers meet the requirements of the Board's information security program.

Continuous Monitoring of Information Security

Implementing a Boardwide information security continuous monitoring (ISCM) program that complies with National Institute for Standards and Technology (NIST) requirements continues to pose challenges to the Board. NIST Special Publication 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, states that the organization-wide ISCM strategy and associated policy should be developed at the organizational tier. The publication also states that at the mission/business processes tier, the organization should establish general procedures for the implementation of the organization's policy, including the minimum frequency with which each security control or metric is to be assessed or monitored.

As noted in recent audits, the Board's Chief Information Officer has made progress in implementing an ISCM program; however, in implementing the program, the Chief Information Officer should determine baseline metrics and define the frequency of monitoring. Additionally, the Board faces challenges in analyzing the ISCM maturity model to determine the Board's optimal target level of implementation and developing mature processes to achieve that level.

Risk Management

Implementing a Boardwide risk management program continues to pose challenges to the Board. Information security risk is the risk associated with the operation and use of information systems that support the mission and business functions of organizations. The Board's information systems house personally identifiable information, market-moving economic data, and other sensitive information that must be adequately protected. Most of the Board's computing environment is managed by the Division of Information Technology (Division of IT); however, some functions are managed within each Board division. NIST requires that the risk management program address and cover all aspects of the Board's computing environments within all divisions' missions and business processes. Similarly, the Federal Information Security Management Act of 2002, as amended by the Federal Information Security Modernization Act of 2014 (FISMA), requires organizations to develop and implement an organization-wide information security program for the information and information systems that support the operations and assets of the organization, including those provided or managed by another organization, a contractor, or another source. NIST Special Publication 800-39, *Managing Information Security Risk*, states that it is imperative that leaders and managers at all levels understand their responsibilities and are held accountable for managing information security risk. Our recent audits noted that the Board's Chief Information Officer has continued to make progress in developing a risk management program; however, the Board will face challenges in implementing the program Boardwide.

Reliance on Third-Party Providers

FISMA requires the Board to ensure that all third-party providers maintain information security in accordance with FISMA requirements. Because the Board relies on third-party providers, including the Federal Reserve Banks, to help carry out its mission effectively, the Board continues to face challenges in ensuring that the third-party providers' information systems and services meet FISMA requirements. Our recent audit work identified that some services provided by third-party providers, including the Reserve Banks, did not meet all the Board's information security requirements.

Agency Actions

The Board's Information Security Officer has made continuous monitoring a priority for the Board by investing in new tools and products to improve the Board's continuous monitoring program. The Information Security Officer informed us that the Board is (1) identifying items to track and metrics against which to track them, (2) working on prioritizing controls for annual testing, and (3) working to use automated methods to conduct the testing. Finally, the Information Security Officer also finalized the *Continuous Monitoring Standard* in October 2014.

The Board uses the *Risk Management Program and Risk Assessment Standard* to enhance the original risk assessment framework initiative. The Chief Information Officer informed us that the IT Enterprise Risk Management processes and procedures have been distributed throughout the Board; these processes and procedures include the identification of all IT-related risks that affect the Board's enterprise IT services and all risks specific to the IT operations hosted within the business divisions and offices.

The Federal Reserve System is currently using the *Security Assurance for the Federal Reserve (SAFR) Policy*, which is based on NIST requirements, as the strategic direction for the Federal Reserve Banks' information security program. This information security program defines the rules, such as the security objectives and control requirements, and the risk management process that help the Federal Reserve System manage information security risk.

The Information Security Officer informed us that the Board treats Federal Reserve System parties differently than other external contractors. The Information Security Officer is creating a trust agreement between the Board and the rest of the Federal Reserve System to rely on the *Security Assurance for the Federal Reserve (SAFR) Policy* as the substantive equivalent to the *Board Information Security Program*. For non–Federal Reserve System external parties, the Information Security Committee has developed a new process for appropriate oversight of third-party vendors. The Chief Information Officer informed us that a new policy, currently undergoing review, will ensure that the information security and information assurance requirements of the Board are included directly in the Board's procurement processes and documentation, including requests for proposals and contracts.

Management Challenge 3: Continuing to Implement a Financial Stability Regulatory and Supervisory Framework

One of the Board's core activities to support its mission is promoting the safety, soundness, and stability of large and complex, as well as smaller, financial institutions and financial market infrastructures. The Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) provides the Board with the authority to oversee nonbank financial companies designated by the Financial Stability Oversight Council as systemically important. This legal authority expands the Board's role in the supervisory oversight of systemically important firms.

As a result of the Dodd-Frank Act and lessons learned during the financial crisis, the Board outlined its updated framework for consolidated supervision of large financial institutions in Supervision and Regulation Letter 12-17. The Board also has developed several policies and implemented supporting guidance to address legislative mandates and further clarify guidance on supervisory expectations. The Board faces challenges in improving the financial sector's ability to withstand future economic downturns and coordinating with other federal supervisory agencies. The following sections describe specific challenges associated with implementing the financial stability regulatory and supervisory framework.

Maintaining Effective Relationships With Other Regulators

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 primary supervisors of holding company subsidiaries. While the Board has taken steps to improve interagency collaboration and cooperation (as described below), continued coordination with other federal supervisory agencies, such as the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency, is crucial to implementing the financial stability regulatory and supervisory framework.

Finalizing and Ensuring Compliance With New Regulations

While the Board has finalized many of the regulations mandated by the Dodd-Frank Act and other significant rulemakings supporting the financial stability framework, some rulemakings remain in the comment phase or have yet to be finalized. For example, the Board has not yet finalized emergency lending regulations under the Dodd-Frank Act. The Board must continue to finalize regulations and develop guidance to address legislative mandates and changes in the economic environment.

Further, the Board faces challenges in coordinating supervision and supporting financial stability as its focus shifts from rulemaking to implementing the rules and ensuring compliance with recently issued regulations. For example, the Volcker Rule took effect in April 2014, but

compliance with requirements of the final rule was not required until July 2015.[2] To hold banks accountable for complying with the final rule, Federal Reserve Bank examiners are expected to monitor and enforce compliance with prohibitions and restrictions related to proprietary trading and certain relationships with hedge funds or private equity funds.

The Board created an executive steering committee, composed of Federal Reserve System staff members, to oversee its supervisory program implementation efforts for the Volcker Rule. To facilitate effective implementation at the Reserve Banks, each Reserve Bank has designated a single point of contact to (1) receive inquiries from Reserve Bank supervision staff and (2) disseminate the responses from Board staff. In April 2015, the Board outlined its expectations for how Reserve Bank staff should handle questions related to the Volcker Rule and how they should provide information to supervised institutions during the conformance period. The Board will continue to monitor its training needs related to the Volcker Rule and already anticipates providing additional training for examiners on this rule in 2015.

Developing Technology Infrastructure

The Board faces challenges in developing analytical tools to support its supervisory programs. Within the large bank portfolio, our evaluation work has revealed that supervisory teams have encountered challenges searching through the large amount of supervisory information that results from the Board's continuous monitoring activities. The Board has taken steps to implement a supervisory data and technology strategy. As a part of this effort, the Board developed the Consolidated Supervision Comparative Analysis, Planning and Execution System (C-SCAPE) application to support the supervisory processes for large banking organizations and to enable continuous monitoring and updates of information from examinations of financial institutions. The Board is currently updating C-SCAPE to match the new framework for the consolidated supervision of large financial institutions. Within the regional and community bank portfolios, the Board is implementing a new system with automated tools to support a common supervisory approach and to increase examination efficiency. The Reserve Banks, however, are in different stages of implementing and using this system. The Board must continue to leverage and fully implement this technology, which will help it to effectively and efficiently conduct its supervision activities and will support continuous monitoring.

Agency Actions

The Board continues to coordinate with supervisory counterparts to align strategic objectives and minimize duplication of efforts. For example, the Board recently implemented formal quarterly interagency meetings with the Federal Deposit Insurance Corporation and the Office of the Comptroller of the Currency to discuss supervisory planning and strategies.

2. On December 18, 2014, the Board extended the conformance period until July 21, 2016, for certain investments in and relationships with covered funds and foreign funds that were in place prior to December 31, 2013 (known as *legacy-covered funds*).

The Board also has made progress in fulfilling the regulatory mandates outlined in the Dodd-Frank Act and in finalizing other rulemakings that support the financial stability framework. For example, the Board issued supervisory guidance to support its updated framework for consolidated supervision of large financial institutions. In Supervision and Regulation Letter 14-8, the Board outlined supervisory expectations for recovery planning at certain large bank holding companies to enhance the resiliency of these firms when responding to adverse developments. In Supervision and Regulation Letter 15-7, the Board provided additional guidance on the governance structure of the Large Institution Supervision Coordinating Committee supervisory program, defining the specific roles and responsibilities of the committees, the subgroups, and the dedicated supervisory teams.

Management Challenge 4: Building and Sustaining a High-Performing and Diverse Workforce

The Board's success in achieving its mission depends on attracting, retaining, and developing a qualified, diverse, and agile workforce. Continually evolving workforce expectations and the highly competitive hiring environment for staff with the specialized skills that the Board needs create challenges for the Board. A key step in ensuring that the Board has a diverse workforce that can effectively carry out the Board's mission is identifying the necessary technical, managerial, and leadership skills through workforce and succession planning. In addition, the Board must continue to support its new performance management process, which is intended to provide greater accountability for organizational objectives and to support employee development.

Recruiting, Engaging, and Retaining a Highly Skilled, Diverse Workforce

The Board faces challenges in recruiting and retaining a highly skilled, diverse workforce due to several factors. The Board must recruit in a competitive hiring environment for individuals with skills in science, technology, engineering, and math. In addition, to retain the highly skilled workforce it needs, the Board must successfully address evolving expectations regarding diversity, workplace flexibility, career progression, communication, and continuous learning.

To better engage its current workforce, the Board administered an employee engagement survey in 2014. To address the survey results, the Board has undertaken initiatives both Boardwide and at the division level to further explore and address staff members' concerns, such as career development and communication. The Board will need to address these concerns to achieve its goal of being a sought-after place to work that attracts highly qualified individuals and embraces the characteristics that each individual brings to the workplace. Effectively employing the unique skills, knowledge, and experiences of the Board's staff members is critical to supporting the innovative thinking that is needed to address the ever-changing environment in which the Board operates.

An important consideration for the Board in recruiting and retaining staff is engaging in workforce planning. The Board will need to determine the required skill sets and number of staff

to enable each division to effectively and efficiently accomplish its goals. In addition, the Board will need to address any skill gaps and align resources to support emerging programs central to the Board's mission. A key part of workforce planning is developing a succession plan to ensure continuity of knowledge and leadership in key positions. Failure to plan for and anticipate turnover and departures could have a negative effect on the Board's ability to achieve its goals and fulfill its mission.

The Board has taken steps to enhance its diversity and inclusion practices; however, our recent audit work identified some improvement opportunities. The Board recognizes that although the representation of minorities among those in line to move into official staff roles has been increasing, it remains low. The Board stated that it has begun to implement processes to track senior-staff position applicant data to be able to better measure trends in diversity. As the Board continues to build and sustain a high-performing and diverse workforce, fostering diversity and inclusion and increasing the representation of minorities among those in line for official staff roles should continue to be areas of focus.

Implementing a New Performance Management System

In 2015, the Board implemented a new performance management system organization-wide following a 2014 pilot program. This new program is intended to strengthen the alignment of expectations for staff members with Board and division strategic goals and responsibilities, provide greater accountability, and support employee development. The new program seeks to be a more forward-looking, development-centric process in which staff members and managers work together for the greater effectiveness of the Board. The Board will be challenged to ensure (1) that the new process is effective, fair, and not overly burdensome and (2) that a consistent approach is followed across the agency. Additionally, the Board's plan to automate the forms for the new performance management system will present further challenges to this new process.

Agency Actions

The Board's first engagement survey was administered in September 2014. The survey was intended to help the Board foster an environment that engages employees in the Board's mission and encourages them to contribute to a positive work environment. Some issues identified by the survey are being addressed at the Board level. In addition, Board divisions have created working groups to address the results of the survey; these efforts are ongoing.

The Board's Organizational Development and Learning section is administering a two-phase, formal agency-wide succession planning program, which began in late 2012, to help identify a diverse pool of candidates for senior management positions throughout the Board. The Board's program will identify development opportunities for employees to prepare them for potential advancement. Both phases are scheduled for full implementation by 2017. Additionally, the Board continues to develop its Leading and

Managing People program, which draws on the expertise of leaders from around the Board to help all Board managers and supervisors develop their skills and strengthen their capacity to identify, coach, and support the future leaders of the organization.

The Board stated that it is finalizing a diversity and inclusion strategic plan and rolling out a new diversity and inclusion scorecard to all Board divisions. Beginning in 2016, the annual scorecards will be assessed by the Office of Minority and Women Inclusion and compiled into one report that will be reviewed by the Board's Chair. The Board also plans to formalize the standards that the Office of Diversity and Inclusion relies on for equal employment opportunity and the racial, ethnic, and gender diversity of the workforce and the senior management of the agency, which will be included in the diversity and inclusion strategic plan.

The Board is updating its performance management policy to better reflect the new performance management system. In addition, the Board contracted for the necessary expertise to assist with the program's implementation, which includes information sessions, tools and guides, training, and other support.

Management Challenge 5: Improving Collaboration and Governance

Aspects of governance, particularly with respect to Boardwide communication and coordination, IT services, data collection and management, and internal control, will continue to pose management challenges to the Board's efficient accomplishment of its mission. While the Board's broad mission remains essentially unchanged, the financial crisis fundamentally changed how the Board operates within its functional disciplines. Accordingly, the Board recognizes the importance of enhanced collaboration within the organization and is enhancing the efficiency and effectiveness of its operations and internal processes through efforts such as strategic planning and budgeting.

Communication and Coordination Across Divisions

Historically, the Board's divisions have operated largely autonomously in performing their specified mission functions, developing organizational structures, formulating budgets, and establishing management processes. For example, a prior OIG audit identified a lack of centralized governance for the Board's continuity of operations program. The Board recognizes the importance of aligning resources to support current and emerging programs that are central to the Board's mission and that establishing a more effective governance system can help it to allocate the appropriate amount and mix of resources to priorities. To achieve that goal, the Board plans to establish a governance system that more effectively prioritizes its available resources.

IT Services

The Board continues to face governance challenges in balancing its centralized and decentralized management of IT services. A primary mission of the Division of IT is to provide services to meet the automation and data analysis needs of the other Board divisions; however, Board divisions also provide IT services to their employees. Our recent follow-up review on recommendations made to the Division of IT found that although the Board's Business Technology Strategic Committee meets to discuss Boardwide issues, it is still challenged to reach the end goal of identifying IT services that can be optimized through centralization and a reduction of duplicative efforts. A key challenge to provisioning IT services in a manner that maximizes efficiency is the implementation of a structured process that ensures that information technology assets deliver business value and are allocated based on overall organizational goals and priorities, and that risks are effectively mitigated.

Data Collection and Management

As a result of expanded responsibilities under the Dodd-Frank Act, the Board is engaging in new data collection and analysis. New data collection and data management processes are required to perform these new responsibilities, and new challenges have emerged in terms of data quantity, quality, access, and controls. Traditionally, data were used within divisions to accomplish specific mission functions; however, to fulfill the Board's expanded responsibilities, divisions now need to increase coordination with each other and with the Board's Office of Financial Stability Policy and Research. A Boardwide data management view is needed to enhance the ability of staff members to obtain, interpret, and analyze these data; however, this is a challenge because of the decentralized nature of some Board operations. The Board also faces challenges in expanding its technology infrastructure and processes to support the increased requests for, and analysis of, data, as well as to enable comprehensive, enterprise-level data governance, policies, procedures, and information management practices.

Maintaining and Monitoring Internal Controls

Internal control is an integral part of managing an organization and is critical to improving organizational effectiveness and accountability. A prior OIG audit found that the Board did not have a Boardwide process for maintaining and monitoring its administrative internal controls and identified other internal control weaknesses at the Board. While these control weaknesses have not prevented the Board from carrying out its mission or achieving its strategic objectives, some have introduced operational and reputational risks and may result in inefficiencies in Board operations. Establishing a process for maintaining and monitoring internal controls will help ensure that the Board's controls, as designed and implemented, are effective, continue to work over time, and provide a means for the Board to identify and timely mitigate control weaknesses.

Agency Actions

The Division of IT holds monthly meetings with the Board's Business Technology Strategic Committee. During these meetings, each Board division discusses the IT services it manages and the corresponding intersection with Boardwide technology and business processes. The Chief Information Officer informed us that the Division of IT, in conjunction with the Business Technology Strategic Committee, is developing a framework to help define the services being provided, to promote efficient resource usage, and to ensure alignment with key business drivers.

In May 2013, the Board established the Office of the Chief Data Officer (OCDO) to centralize data governance across the divisions. The OCDO established an Enterprise Data Governance Framework, based on industry best practices, that consists of three themes that describe the components of enterprise data governance. The OCDO has also created a road map and a detailed operating plan for 2015–2016 that includes strategies and initiatives for launching the data governance program. Further, in an effort to coordinate and communicate data management matters across the Board's business and technology operations and functions, the OCDO reconstituted the Board Data Council. The council is chartered to provide strategic advisory services to the OCDO for Board data governance program goals, policies, and execution. The council also endorses, approves, and authorizes OCDO-developed data governance and data management policies, processes, definitions, standards, and metrics to be implemented across the Board's data environment.

Board management identified several planned actions to enable effective implementation of strategic themes and to address governance challenges. Specifically, the Board established workgroups made up of senior leaders representing all the Board's divisions and offices to develop objectives and performance indicators for the Board's strategic plan. To support effective project management for significant projects, the Board has established an Investment Review Board and integrated it into the budget and strategic reporting process. Finally, Board management is drafting a policy and procedures document to be used by all divisions in implementing a Boardwide internal control program. A pilot of this process is underway, and the Division of Financial Management is working with several other divisions to develop a plan to implement the internal control program.

Management Challenge 6: Maintaining Physical Infrastructure

Successfully renovating the William McChesney Martin, Jr., Building (Martin Building) is a long-term goal of the Board. The Martin Building facility has not been significantly renovated since its construction in 1974. In addition to ensuring a safe and adequate environment in which individuals and groups can work and meet, efforts associated with the renovation will focus on security, energy efficiency, meeting and conference space, and physical plant capacity. It is a multiyear project that poses challenges due to its size, complexity, and effect on the Board's staff members. While managing the renovation effort, the Board will also need to

manage its space planning and leasing activities to accommodate staff members displaced during the renovation as well as ongoing staff growth.

Martin Building Renovation

The Martin Building renovation project is the Board's largest contracting effort. Since the original concept was developed, the project has gone through a lengthy design phase. Further delays during renovation could lead to increased costs for the Board. Many parties are involved in the renovation process, and interdependencies exist. As a result, delays could cascade and affect the timing and sequencing of others' work. Project management has been complicated by changes in the Board's organizational structure and leadership. The renovation has significant implementation risks and challenges that the Board must manage, including scope changes, contractor oversight, cost management, asset tracking, and disruption to staff members.

Space Planning and Leasing

The Board currently occupies space in several buildings in Washington, DC. The Board's overall staffing level has grown significantly over the last several years, and continued growth is expected in some of its divisions. Over the past year, the Board has been moving employees to accommodate overall staff growth as well as staff displacement due to the Martin Building renovation.

The Board is challenged with accommodating the expected growth of its workforce while also effectively managing its existing real property assets. The management of federal real property was identified as a high risk by the U.S. Government Accountability Office. The Board acknowledges the need to focus on its long-term space requirements while also considering, in the context of its strategic framework, factors such as the current space environment, building location limitations, the projected growth of the organization, technological requirements, the implications of telework, and the operational effects and life cycle costs of all options.

Agency Actions

The Board has been increasing the number of personnel involved in managing the Martin Building renovation and in moving staff to alternate locations. Further, since 2011, the Board has hired personnel with construction experience. In addition to the project team, an executive team and the Executive Oversight Group were established to be strategic advisors to the Martin Building renovation project. As of July 2015, the Board had moved approximately 600 staff members out of the Martin Building and into owned or leased space around Washington, DC. It will continue to move staff members out of the Martin Building during 2015.

Recognizing that it needs to take a more consistent approach to space planning, the Board is developing a standard process for allocating and managing its space. The

Board is also developing a strategic master plan for space planning, and it contracted for real estate advisory services to assist with this effort. The plan is intended to inform senior leadership decisions regarding the Board's space needs.

Closing

We appreciate the cooperation that we received from the Board regarding this year's major management challenges. Please contact me if you would like to discuss any of the challenges.

cc: Scott G. Alvarez, General Counsel, Legal Division
Eric Belsky, Director, Division of Consumer and Community Affairs
Michell Clark, Director, Management Division
Robert Frierson, Secretary of the Board, Office of the Secretary
Michael Gibson, Director, Division of Banking Supervision and Regulation
Donald Hammond, Chief Operating Officer, Office of the Chief Operating Officer
Steven Kamin, Director, Division of International Finance
Thomas Laubach, Director, Division of Monetary Affairs
J. Nellie Liang, Director, Office of Financial Stability Policy and Research
William Mitchell, Chief Financial Officer and Director, Division of Financial Management
Sharon Mowry, Chief Information Officer and Director, Division of Information Technology
Louise Roseman, Director, Division of Reserve Bank Operations and Payment Systems
Michelle Smith, Assistant to the Board, Chief of Staff, and Director, Office of Board Members
David Wilcox, Director, Division of Research and Statistics