Office of Inspector General

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

Semiannual Report to Congress

October 1, 2018–March 31, 2019

OIG

Semiannual Report to Congress

October 1, 2018–March 31, 2019

Office of Inspector General

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

Message From the Inspector General

Since our previous semiannual report to Congress, new leaders have joined both of the agencies we oversee. Kathy Kraninger became Director of the Bureau of Consumer Financial Protection (Bureau), and Michelle Bowman took office as a member of the Board of Governors of the Federal Reserve System (Board). We've met with Director Kraninger and Governor Bowman, and we look forward to continuing to work with leadership at the Board and the Bureau as we provide independent oversight to improve their programs and operations and to prevent and detect fraud, waste, and abuse.

During the past 6 months, we issued eight reports related to the Board's programs. These reports address information security, information technology governance, the shipment of currency, academic assistance, audits of financial statements, and workforce planning. We issued four reports on the Bureau's operations, which examine information security, purchase card controls, the monitoring of corrective actions at supervised institutions, and the scheduling of examination activities.

Our Office of Investigations pursued allegations of fraud against Board and Bureau supervision programs as well as allegations of wrongdoing concerning our agencies' internal operations. We processed 262 new hotline complaints and closed 13 investigations, and our work resulted in 10 persons referred for criminal prosecution and more than $1.3 billion in criminal fines, restitution, and special assessments. Of note were the sentencings of four former Wilmington Trust executives to imprisonment for fraud, false entries, and false statements as well as Société Générale S.A.'s agreement to pay more than $1.3 billion in monetary penalties for its willful violation of U.S. economic sanctions.

Although our work focuses on the programs and operations of the Board and the Bureau, our findings often have applicability beyond our specific agencies. To help share this knowledge with other organizations, we issued our second OIG Insights paper in February. In this paper, we summarize five strategies organizations can use to strengthen their organizational governance system, including adapting governance processes and structures to fit their organizational needs and ensuring transparency to stakeholders.

We actively engage with and seek input from a variety of stakeholders. Over the past 6 months, we met with key members of our oversight committees, hosted conferences to foster cooperation among our law enforcement partners, and engaged with staff throughout the Board and the Bureau so that we are able to provide timely and insightful oversight of Board and Bureau programs and operations.

I am proud that the Office of Inspector General continues to be a force for positive change. We welcomed Fred W. Gibson, Jr., as Deputy Inspector General in November, and I look forward to his outstanding contributions. I am also profoundly grateful for the professionalism and expertise of every member of the Office of Inspector General staff, whose dedication, commitment, and high-quality work make it possible for us to fulfill our mission.

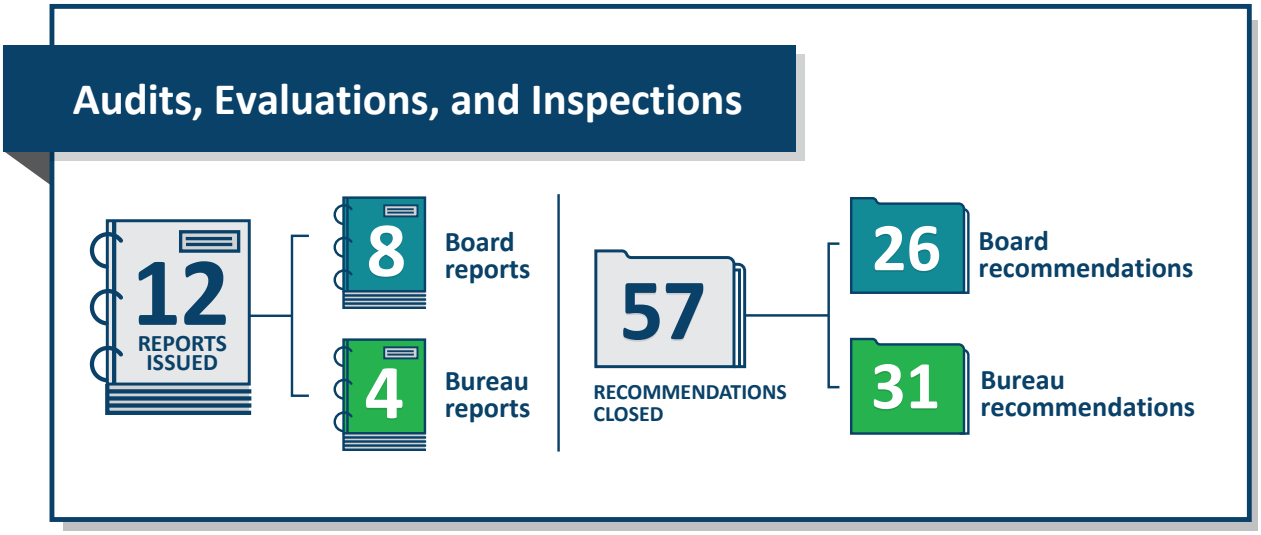
Sincerely,

Mark Bialek
Inspector General
April 30, 2019

Contents

Highlights

We continued to promote the integrity, economy, efficiency, and effectiveness of the programs and operations of the Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection (Bureau). The following are highlights of our work during this semiannual reporting period.



The Board's Information Security Program

The Board's information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security. The Board has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five security functions outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

The Bureau's Information Security Program

The Bureau's information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. The Bureau has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program is effective.

The Board's Governance of Information Technology

Certain aspects of the Board's organizational structure and authorities could inhibit the Board's achievement of its strategic objectives regarding technology as well as its achievement of an effective FISMA maturity rating. Although the Board has information technology (IT) governance mechanisms in place, we found opportunities for improvement in the areas of security, budgeting, procurement, and capital planning.

The Bureau's Follow-Up Process for Matters Requiring Attention

During the examination process, Bureau employees may identify corrective actions that a supervised institution needs to implement to address certain violations, deficiencies, or weaknesses. These corrective actions include Matters Requiring Attention (MRAs). The Bureau can improve its follow-up process for MRAs.

Strengthening Organizational Governance

Organizational governance involves processes and structures for decisionmaking, accountability, controls, and behaviors designed to accomplish an organization's objectives. A strong governance system can enable an organization to achieve its objectives more efficiently and effectively. This OIG Insights paper summarizes insights from our 2017 evaluation of the Board's organizational governance more broadly, highlighting practices and considerations that other organizations can use to strengthen their governance system.

The Board's Workforce Planning

Board division leaders have varying perspectives on the need for an enterprisewide workforce planning process, and their buy-in to participate in such a process may be impeded by factors including communication, undefined roles and responsibilities, a lack of clear support from top Board leaders, and existing division-specific approaches to workforce planning.

The Bureau's Risk Assessment Framework for Examinations

We identified opportunities for the Bureau to improve its risk assessment framework for prioritizing and scheduling examinations, which includes the identification, analysis, and prioritization of specific institution product lines for examination.

Former Wilmington Trust Executives Sentenced in Federal District Court

Four former executives of Wilmington Trust Bank were sentenced to incarceration ranging from 36 to 72 months, a total of $700,000 in fines, and prohibition from banking. The executives were found guilty of conspiracy to defraud the United States, securities fraud, making false statements in documents required to be filed with the U.S. Securities and Exchange Commission (SEC), making false entries in banking records, and making false statements to the SEC and to the Board.

Criminal Charges Against Société Générale S.A.

On November 19, 2018, the U.S. Attorney's Office for the Southern District of New York announced criminal charges against Société Générale S.A. (SG) consisting of a one-count felony information charging SG with conspiring to violate the Trading with the Enemy Act and the Cuban Asset Control Regulations for SG's role in processing billions of dollars of U.S. dollar transactions using the U.S. financial system, in connection with credit facilities involving Cuba. Under a deferred prosecution agreement, SG agreed

to pay $1.34 billion in penalties—the second-largest penalty ever imposed on a financial institution for violations of U.S. economic sanctions.

Former Acting President of CFG Community Bank Sentenced to Federal Prison for Bank Fraud and Tax Evasion

A former acting President of CFG Community Bank, a state member bank, was sentenced to 3 years in federal prison for bank fraud and tax evasion. The defendant was also ordered to pay $892,541.75 in restitution to CFG and $365,228.80 in restitution to the Internal Revenue Service and to forfeit $503,378.87.

Introduction

Established by Congress, we are the independent oversight authority for the Board and the Bureau. In fulfilling this responsibility, we conduct audits, evaluations, investigations, and other reviews related to Board and Bureau programs and operations. By law, Offices of Inspector General (OIGs) are not authorized to perform agency program functions.

In accordance with the Inspector General Act of 1978, as amended (5 U.S.C. app. 3), our office has the following responsibilities:

- conduct and supervise independent and objective audits, evaluations, investigations, and other reviews to promote economy, efficiency, and effectiveness in Board and Bureau programs and operations
- help prevent and detect fraud, waste, abuse, and mismanagement in Board and Bureau programs and operations
- review existing and proposed legislation and regulations to make recommendations about possible improvements to Board and Bureau programs and operations
- keep the Board of Governors, the Bureau Director, and Congress fully and currently informed

Congress has also mandated additional responsibilities that influence our priorities, including the following:

- Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act; 12 U.S.C. § 1831o(k)), requires that we review and report within 6 months on Board-supervised financial institutions whose failure results in a material loss to the Deposit Insurance Fund (DIF). Section 38(k) also requires that we conduct an in-depth review of any nonmaterial losses to the DIF that exhibit unusual circumstances.
- The Federal Reserve Act, as amended by the USA PATRIOT Act of 2001 (12 U.S.C. § 248(q)), grants the Board certain federal law enforcement authorities. We perform the external oversight function for the Board's law enforcement program.
- FISMA (44 U.S.C. § 3555) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In accordance with FISMA requirements, we perform annual independent reviews of the Board's and the Bureau's information security programs and practices, including the effectiveness of security controls and practices for selected information systems.

- The Improper Payments Information Act of 2002, as amended (IPIA; 31 U.S.C. § 3321 note), requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to IPIA. The Improper Payments Elimination and Recovery Act of 2010 requires us to determine each fiscal year whether the agency is in compliance with IPIA.
- Section 211(f) of the Dodd-Frank Act (12 U.S.C. § 5391(f)) requires that we review and report on the Board's supervision of any covered financial company that is placed into receivership. We are to evaluate the effectiveness of the Board's supervision, identify any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommend appropriate administrative or legislative action.
- Section 989E of the Dodd-Frank Act (5 U.S.C. app. 3 § 11 note) established the Council of Inspectors General on Financial Oversight (CIGFO), which is required to meet at least quarterly to share information and discuss the ongoing work of each Inspector General (IG), with a focus on concerns that may apply to the broader financial sector and ways to improve financial oversight.[1] Additionally, CIGFO must report annually about the IGs' concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO can also convene a working group of its members to evaluate the effectiveness and internal operations of the Financial Stability Oversight Council, which was created by the Dodd-Frank Act and is charged with identifying threats to the nation's financial stability, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system.
- The Government Charge Card Abuse Prevention Act of 2012 (5 U.S.C. § 5701 note and 41 U.S.C. § 1909(d)) requires us to conduct periodic risk assessments and audits of the Bureau's purchase card, convenience check, and travel card programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments.
- Section 11B of the Federal Reserve Act (12 U.S.C. § 248(b)) mandates annual independent audits of the financial statements of each Federal Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we oversee the annual financial statement audits of the Board and of the FFIEC.[2] Under the Dodd-Frank Act, the U.S. Government Accountability Office performs the financial statement audit of the Bureau.

1. CIGFO comprises the IGs of the Board and the Bureau, the Commodity Futures Trading Commission, the U.S. Department of Housing and Urban Development, the U.S. Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, the SEC, and the Office of the Special Inspector General for the Troubled Asset Relief Program.

2. The FFIEC is a formal interagency body empowered (1) to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the Bureau and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

- The Digital Accountability and Transparency Act of 2014 (DATA Act; 31 U.S.C. § 6101 note) requires agencies to report financial and payment data in accordance with data standards established by the U.S. Department of the Treasury (Treasury) and the Office of Management and Budget. The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to the DATA Act and that only one specific DATA Act requirement, section 3(b), applies to the Bureau Fund. The DATA Act requires us to review a statistically valid sample of the data submitted by the agency and report on its completeness, timeliness, quality, and accuracy and on the agency's implementation and use of the data standards.

Audits, Evaluations, and Inspections

Audits assess aspects of the economy, efficiency, and effectiveness of Board and Bureau programs and operations. For example, we oversee audits of the Board's financial statements and conduct audits of (1) the efficiency and effectiveness of the Board's and the Bureau's processes and internal controls over their programs and operations; (2) the adequacy of controls and security measures governing these agencies' financial and management information systems and their safeguarding of assets and sensitive information; and (3) compliance with applicable laws and regulations related to the agencies' financial, administrative, and program operations. Our audits are performed in accordance with the *Government Auditing Standards* established by the Comptroller General of the United States.

Evaluations and inspections include program evaluations and legislatively mandated reviews of failed financial institutions supervised by the Board. Evaluations are generally focused on the effectiveness of specific programs or functions. Inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Our evaluations and inspections are performed according to the *Quality Standards for Inspection and Evaluation* issued by the Council of the Inspectors General on Integrity and Efficiency (CIGIE).

The information below summarizes our audit and evaluation work completed during the reporting period.

Board of Governors of the Federal Reserve System

2018 Audit of the Board's Information Security Program

2018-IT-B-017 **October 31, 2018**

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Board. We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Board's information security program is operating at a level-4 (*managed and measurable*) maturity, which indicates an overall effective level of security. The Board has opportunities to mature its information security program in FISMA domains across all five security functions outlined in the National Institute of Standards and Technology's Framework for Improving Critical Infrastructure Cybersecurity—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. A consistent theme is that the lack of an agencywide risk-management governance structure and strategy, as well as the decentralization of IT services, results in an incomplete view of the risks affecting the Board's

security posture. Although the Board has taken steps to move toward an agencywide approach to risk management governance and IT services, several security processes, such as asset management and enterprise architecture, have not yet been implemented agencywide.

The Board had taken sufficient action to close 4 of the 13 recommendations from our prior FISMA audits that remained open at the start of this audit. We made 6 new recommendations designed to strengthen the Board's information security program in the areas of risk management, configuration management, data protection and privacy, and security training. The Board concurred with our recommendations.

Evaluation of the Board's Implementation of Splunk

2018-IT-B-019R **November 5, 2018**

The Splunk system is the Board's primary security information and event management application. We evaluated the Board's implementation of Splunk in accordance with security best practices as well as the system's compliance with FISMA and the Board's information security policies, procedures, standards, and guidelines.

Overall, we found the Board implemented Splunk in line with security best practices. For example, Splunk forwarders are consistently installed on Board devices, and dashboards have been developed and implemented to monitor and validate that the agency's devices are forwarding data to Splunk correctly. However, we identified an opportunity to strengthen risk management controls.

Our report contains one recommendation to strengthen security as well as three matters for management's consideration related to account management, annual access validation, and self-signed certificates. The Board concurred with our recommendation and outlined corrective actions to address the issues we identified.

The Board Can Strengthen Information Technology Governance

2018-IT-B-020 **November 5, 2018**

The efficiency and effectiveness of the Board's agencywide information security program is contingent on enterprisewide visibility into IT operations. As part of our requirements under FISMA, we assessed whether the Board's current organizational structure and authorities support its IT needs—specifically, the organizational structure and authorities associated with security, privacy, capital planning, budgeting, and acquisition.

Overall, we found that certain aspects of the Board's organizational structure and authorities could inhibit the Board's achievement of its strategic objectives regarding technology as well as its achievement of an

effective FISMA maturity rating. Although the Board has IT governance mechanisms in place, we found opportunities for improvement in the areas of security, budgeting, procurement, and capital planning.

First, the Chief Information Officer may not have appropriate visibility into all IT decisions made at the Board. The Board's *Delegations of Administrative Authority* authorizes Board Division Directors to make independent IT investment decisions for their divisions, and divisions are not required to align their IT investments with the Board's enterprisewide architecture. Second, the Board lacks a documented reporting hierarchy and authority structure for its various IT governance boards and committees, and the Investment Review Board lacks a mechanism to elevate concerns with an IT project to those with the authority to pause or cancel the project. Third, Board divisions are not consistently tracking labor hours for the purpose of capitalizing software development costs. Therefore, the capitalized costs for the Board's internally developed software assets may be inaccurate.

Our report contains recommendations designed to strengthen IT governance at the Board. The Board concurred with our recommendations.

The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration

2018-FMIC-B-021 **December 3, 2018**

The Board's Banknote Issuance and Cash Operations section is responsible for the currency shipment process. This process includes monitoring and forecasting the demand for currency and planning and executing the issuance of currency to Reserve Bank cash offices. We assessed the efficiency and effectiveness of the Board's management of the currency shipment process and the effectiveness of related contracting activities.

The Board's currency shipment process is generally effective; however, the process can be enhanced to gain time and cost efficiencies. Streamlining the currency forecasting process could save time and minimize the potential for human error. Selecting different transportation modes for certain currency shipment routes and evaluating alternatives to transporting shipping equipment could yield transportation cost savings.

Additionally, the Board can improve the administration of its armored carrier contracts to help ensure that the Board is adequately protected against loss or damage during shipments, that armored carriers are adequately protecting Board data, and that the Board is receiving the expected level of service.

Our report contains recommendations designed to help the Board seek additional efficiencies in the currency shipment process and to improve the administration of armored carrier contracts. The Board concurred with our recommendations.

The Board Can Strengthen Controls Over Its Academic Assistance Program

2018-MO-B-023 December 12, 2018

The Board maintains an academic assistance program and encourages employees to use the program to enhance their development and support their career progression. Employees who qualify may receive up to $12,200 per calendar year in academic assistance. We assessed the adequacy of the internal controls related to the management and administration of the Board's academic assistance program.

The Board can strengthen controls over its academic assistance program. Specifically, the Board should strengthen controls over the program's application processes. We found that certain documentation was not maintained and complete application information was not submitted prior to approving reimbursement. We also found that the Board did not consistently monitor employees' timely submission of course grades. The Board should also improve its *Academic Assistance* policy, procedures, and application form to include a requirement that program participants submit proof of actual costs being reimbursed as well as receipt of any outside educational assistance. Lastly, we found that the Board should improve the *Academic Assistance* policy to ensure consistency with related guidance and to clarify what qualifies as an allowable expense.

The Board is in the process of improving its academic assistance program, including developing automated features to process academic assistance applications and to monitor compliance with annual academic assistance limits. We did not audit the automated features because they were under development at the time of our audit and therefore outside our scope of review.

Our report contains recommendations designed to strengthen controls over the Board's academic assistance program processes. The Board concurred with our recommendations.

Strengthening Organizational Governance

OIG Insights February 14, 2019

In a 2017 report,[3] we recommended ways for the Board to improve its organizational governance system. In this paper, we summarize insights from that evaluation more broadly. Organizational governance involves processes and structures for decisionmaking, accountability, controls, and behaviors designed to accomplish an organization's objectives. A strong governance system can enable an organization to achieve its objectives more efficiently and effectively.

Organizations that want to strengthen their governance system should (1) adapt governance processes and structures to fit organizational needs; (2) define and communicate delegated roles, responsibilities, and

3. Office of Inspector General, *The Board's Organizational Governance System Can Be Strengthened*, OIG Report 2017-FMIC-B-020, December 11, 2017.

authorities; (3) set expectations for internal communication; (4) ensure transparency to stakeholders; and (5) periodically review the organizational governance system.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2018 and 2017, and Independent Auditors' Reports

2019-FMIC-B-002 **February 27, 2019**

The Board performs the accounting function for the FFIEC, and we contract with an independent public accounting firm to annually audit the financial statements of the FFIEC. The contract requires the audits to be performed in accordance with auditing standards generally accepted in the United States of America and in accordance with the auditing standards applicable to financial audits in the *Government Auditing Standards* issued by the U.S. Comptroller General. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the FFIEC as of December 31, 2018 and 2017, and the results of operations and cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America. The auditors' report on internal control over financial reporting and on compliance and other matters disclosed no instances of noncompliance or other matters.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2018 and 2017, and Independent Auditors' Reports

2019-FMIC-B-003 **March 7, 2019**

We contracted with an independent public accounting firm to audit the financial statements of the Board and to audit the Board's internal control over financial reporting. The contract requires the audits of the financial statements to be performed in accordance with the auditing standards generally accepted in the United States of America, the standards applicable to financial audits in the *Government Auditing Standards* issued by the U.S. Comptroller General, and the auditing standards of the Public Company Accounting Oversight Board. The contract also requires the audit of internal control over financial reporting to be performed in accordance with the attestation standards established by the American Institute of Certified Public Accountants and with the auditing standards of the Public Company Accounting Oversight Board. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2018 and 2017, and the results of its operations and its cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America. Also, in the auditors' opinion, the Board maintained, in all material respects, effective internal control over financial reporting as of December 31, 2018, based on the criteria established in *Internal Control—Integrated Framework* (2013) by the Committee of Sponsoring Organizations of the Treadway Commission. The auditors' report on compliance and other matters disclosed no instances of noncompliance or other matters.

The Board Can Take Additional Steps to Advance Workforce Planning

2019-MO-B-004 **March 25, 2019**

Workforce planning is the systematic process for identifying and addressing the gaps between the workforce of today and the human capital needs of tomorrow. In its *Strategic Plan 2016–19*, the Board identifies its workforce as a strategic priority. Further, the Board has identified developing its workforce planning capability as one way in which it can meet this priority. We assessed the status of enterprisewide workforce planning and related developments at the Board.

The Board's Human Resources function developed a preliminary enterprisewide workforce planning process in 2017 and began piloting it in 2018. Board division leaders have varying perspectives on the need for an enterprisewide workforce planning process, and their buy-in to participate in such a process may be impeded by several factors. These factors include limited initial communication from Human Resources to divisions on Human Resources' preliminary enterprisewide workforce planning process, the need for defined roles and responsibilities, a lack of clear support from top Board leaders, and existing division-specific approaches to workforce planning. As a result, the Board may struggle to advance its workforce planning strategy in all divisions.

The Board can consider further applying common workforce planning principles as it advances its enterprisewide workforce planning process. Although some of the common principles are already incorporated into the Board's workforce planning efforts, we found that a few principles, such as those dealing with coordinating on an enterprisewide level and dedicating appropriate resources, can be further incorporated.

Our report contains recommendations designed to assist the Board in establishing a policy for enterprisewide workforce planning and achieving increased buy-in from division leaders and other stakeholders for such a policy. The Board concurred with our recommendations.

Bureau of Consumer Financial Protection

2018 Audit of the Bureau's Information Security Program

2018-IT-C-018 **October 31, 2018**

To meet our annual FISMA reporting responsibilities, we reviewed the information security program and practices of the Bureau. We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices.

The Bureau's information security program is operating at a level-3 (*consistently implemented*) maturity, with the agency performing several activities indicative of a higher maturity level. The Bureau also has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program is effective. Specifically, the agency can strengthen its enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels. The Bureau can also improve its processes related to database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems. Further, access to one of the Bureau's internal collaboration tools, which contains sensitive information (including personally identifiable information), was not restricted to individuals with a need to know.

The Bureau has taken sufficient action to close 3 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. We made 4 new recommendations designed to strengthen the Bureau's information security program in the areas of configuration management, identity and access management, and data protection and privacy. The Bureau concurred with our recommendations.

Bureau Purchase Card Program Controls Appear to Be Operating Effectively

2018-FMIC-C-022 **December 12, 2018**

The Bureau's purchase card program supports its procurement needs and reduces the administrative cost of purchasing small-dollar items. For the scope of our audit, April 1, 2017, through June 30, 2018, cardholders made about 4,200 transactions, totaling $2.7 million. We assessed whether the controls for the Bureau's purchase card program were adequate (1) to ensure that purchase card use is appropriate and in compliance with applicable laws, regulations, and the Bureau's policies and procedures and (2) to prevent and detect improper or fraudulent use of purchase cards.

The Bureau's purchase card program controls appear to be operating effectively to ensure that purchase card use is appropriate and in compliance with applicable laws, regulations, and internal policies and procedures. In addition, the controls appear to be operating effectively to prevent and detect potentially

improper or fraudulent use of purchase cards. The Bureau's Office of Procurement has established effective controls to minimize risk within the purchase card program, and the Agency/Organization Program Coordinator's oversight of the program helps to ensure compliance with applicable laws, regulations, and internal policies and procedures. We did not make recommendations.

The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions

2019-SR-C-001 **January 28, 2019**

During the examination process, Division of Supervision, Enforcement and Fair Lending (SEFL) employees may identify corrective actions that a supervised institution needs to implement to address certain violations, deficiencies, or weaknesses. These corrective actions include MRAs. We assessed SEFL's effectiveness in monitoring MRAs and ensuring that supervised institutions address them in a timely manner.

SEFL can improve its follow-up process for MRAs. For example, we found that the Bureau's approach for measuring how timely it resolves MRAs is prone to misinterpretation and therefore appeared to overstate the agency's progress toward closing these actions. We also determined that some of the underlying data used to calculate the measurement were not reliable. Additionally, we observed inconsistent MRA follow-up documentation and workpaper retention practices in certain areas.

Our report contains recommendations designed to further enhance the MRA follow-up process. The Bureau concurred with our recommendations.

The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities

2019-SR-C-005 **March 25, 2019**

The scope of the Bureau's financial institution oversight authorities covers depository institutions with more than $10 billion in total assets and thousands of nondepository institutions. The Bureau seeks to prioritize its examination activities based on an annual assessment of the risks that the products offered by these financial institutions present to consumers. We assessed the effectiveness of SEFL's risk assessment framework, including the identification, analysis, and prioritization of specific institution product lines for examination, and we reviewed each region's implementation of the results of the prioritization process through examination scheduling.

We identified opportunities for the Bureau to improve its risk assessment framework for prioritizing and scheduling examinations. Specifically, SEFL's approach for assigning a key risk score to individual institution

product lines is not transparent for some Bureau employees involved in the scoring process; these employees would benefit from additional training and guidance on that process. We also found that SEFL can improve its preliminary research on supervised institutions. Finally, we found that SEFL can improve the internal reporting of changes to the examination schedule.

Our report contains recommendations designed to improve the Bureau's risk assessment framework for prioritizing and scheduling examination activities. The Bureau concurred with our recommendations.

Failed State Member Bank Reviews

Material Loss Reviews

Section 38(k) of the Federal Deposit Insurance Act, as amended, requires that the IG of the appropriate federal banking agency complete a review of the agency's supervision of a failed institution and issue a report within 6 months of notification from the Federal Deposit Insurance Corporation (FDIC) OIG that the projected loss to the DIF is material. Section 38(k) defines a material loss to the DIF as an estimated loss in excess of $50 million.

The material loss review provisions of section 38(k) require that the IG do the following:

- review the institution's supervision, including the agency's implementation of prompt corrective action
- ascertain why the institution's problems resulted in a material loss to the DIF
- make recommendations for preventing any such loss in the future

No state member bank failures occurred during the reporting period that required us to initiate a material loss review.

Nonmaterial Loss Reviews

The Federal Deposit Insurance Act, as amended, requires the IG of the appropriate federal banking agency to semiannually report certain information on financial institutions that incur nonmaterial losses to the DIF and that fail during the 6-month period.

When bank failures result in nonmaterial losses to the DIF, the IG must determine (1) the grounds identified by the federal banking agency or the state bank supervisor for appointing the FDIC as receiver and (2) whether the losses to the DIF present unusual circumstances that would warrant in-depth reviews. Generally, the in-depth review process is the same as that for material loss reviews, but in-depth reviews are not subject to the 6-month reporting deadline.

The IG must semiannually report the completion dates for each such review. If an in-depth review is not warranted, the IG is required to explain this determination. In general, we consider a loss to the DIF to present unusual circumstances if the conditions associated with the bank's deterioration, ultimate closure,

and supervision were not addressed in any of our prior bank failure reports, or if there was potential fraud.

No state member bank failures occurred during the reporting period that required us to initiate a nonmaterial loss review.

Table 1. Nonmaterial State Member Bank Failure During the Reporting Period

State member bank	Location	Asset size (millions)	DIF projected loss (millions)	Closure date	OIG summary of state's grounds for receivership	OIG determination
No nonmaterial state member bank failures occurred during the reporting period.						

Investigations

Our Office of Investigations investigates criminal, civil, and administrative wrongdoing by Board and Bureau employees as well as alleged misconduct or criminal activity that affects the Board's or the Bureau's ability to effectively supervise and regulate the financial community. We operate under statutory law enforcement authority granted by the U.S. Attorney General, which vests our Special Agents with the authority to carry firearms, to seek and execute search and arrest warrants, and to make arrests without a warrant in certain circumstances. Our investigations are conducted in compliance with CIGIE's *Quality Standards for Investigations* and the *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority*.

During this period, the Office of Investigations met with officials at both the Board and the Bureau to discuss investigative operations and the investigative process. The office also met with other financial regulatory agency OIGs to discuss matters of mutual interest, joint investigative operations, joint training opportunities, and hotline operations.

Board of Governors of the Federal Reserve System

The Board is responsible for consolidated supervision of bank holding companies, including financial holding companies formed under the Gramm-Leach-Bliley Act. The Board also supervises state-chartered banks that are members of the Federal Reserve System. Under delegated authority from the Board, the Reserve Banks supervise bank holding companies and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities.

Our office's investigations concerning bank holding companies and state member banks typically involve allegations that senior officials falsified financial records, lied to or misled examiners, or obstructed examinations in a manner that may have hindered the Board's ability to carry out its supervisory operations. Such activity may result in criminal violations, including false statements or obstruction of bank examinations. The following are examples from this reporting period of investigations into matters affecting the Board's ability to carry out its supervisory responsibilities.

Former General Counsel Charged, Borrower Pleaded Guilty, in Conspiracies to Defraud First NBC Bank

The former General Counsel for First NBC Bank, a New Orleans–based bank that failed in April 2017, was charged with conspiracy to commit bank fraud in the U.S. District Court for the Eastern District of

Louisiana. The bank was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company.

The General Counsel worked at First NBC Bank from about 2006 to 2016, during which time he and several businesses he owned or controlled received loans from the bank. A bank President, bank officer, and others conspired to provide First NBC Bank with fraudulent documents that overstated the value and understated liabilities of the General Counsel's and his businesses' assets. These individuals also extended the maturity dates of the loans and issued new loans, including through straw borrowers, giving the appearance that older loans were paid to avoid the bank's downgrading and reporting the loans as losses. In addition, the individuals funded fraudulent tax credit investments from the bank that were actually diverted to the General Counsel and his businesses.

By April 2017, First NBC Bank had advanced about $46 million to the General Counsel and his businesses. The bank also paid the General Counsel an additional $9.6 million dollars in false tax credit investment money. If found guilty, the General Counsel could face up to 30 years' imprisonment, a fine of more than $1 million, 5 years' supervised release, and a special assessment of $100.

Another individual, a borrower of First NBC Bank, pleaded guilty to one count of conspiracy to commit bank fraud. According to the court documents, this defendant, at the direction of the same bank President, submitted false financial statements and inflated accounts receivable to justify incremental increases on a line of credit the defendant received from First NBC Bank. The President caused these false supporting documents to be placed in First NBC Bank's records.

This conspiracy allowed the defendant, the President, and others to unjustly enrich themselves, disguise the defendant's true financial status, and conceal the accurate performance of the defendant's line of credit. The defendant, the President, and others sought to obtain money from First NBC Bank, in part so that the President could continue using the defendant on projects involving a company co-owned by the President without having to use the President's funds to pay the defendant for work on the projects.

This is a joint investigation by our office, the Federal Bureau of Investigation (FBI), and the FDIC OIG and is being prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

Four Former Senior Executives of Wilmington Trust Sentenced in Federal District Court

Four former executives of Wilmington Trust Bank—the President and Chief Operating Officer, the Executive Vice President and Chief Financial Officer, the Chief Credit Officer, and the Controller—were sentenced in U.S. District Court for the District of Delaware. Two of the executives each received a sentence of 72 months' incarceration, 3 years' supervised release, a requirement to enter into a consent

order with the Board for removal and prohibition from banking, and a fine of $300,000. One of the other executives received 54 months' incarceration, 3 years' supervised release, a requirement to enter into a consent order with the Board for removal and prohibition from banking, and a fine of $100,000. The remaining executive received 36 months' incarceration and a requirement to enter into a consent order with the Board for removal and prohibition from banking.

The sentences were based on previous convictions by a jury that found all four defendants guilty of conspiracy to defraud the United States, securities fraud, making false statements in documents required to be filed with the SEC, making false entries in banking records, and making false statements to the SEC and to the Board. The jury also found the Executive Vice President and Chief Financial Officer guilty of making false certifications in financial reports.

According to court documents, the bank was required to report in its quarterly filings with both the SEC and the Board the quantity of its loans for which payment was past due for 90 days or more. The defendants conspired to conceal the truth about the health of Wilmington Trust's loan portfolio from bank regulators, the SEC, and the investing public. The defendants participated in Wilmington Trust's failure to include in its reporting a material quantity of past-due loans, despite the reporting requirements and knowing the significance of past-due loan volume to investors and regulators.

This case was investigated by our office, the FBI, Internal Revenue Service–Criminal Investigation (IRS–CI), and the Office of the Special Inspector General for the Troubled Asset Relief Program.

Manhattan U.S. Attorney Announced Criminal Charges Against Société Générale S.A.

On November 19, 2018, the U.S. Attorney's Office for the Southern District of New York announced criminal charges against SG consisting of a one-count felony information charging SG with conspiring to violate the Trading with the Enemy Act and the Cuban Asset Control Regulations for SG's role in processing billions of dollars of U.S. dollar transactions using the U.S. financial system, in connection with credit facilities involving Cuba. The U.S. Attorney's Office also announced a deferred prosecution agreement under which SG agreed to accept responsibility for its conduct by stipulating to the accuracy of an extensive Statement of Facts, pay penalties totaling $1.34 billion to federal and state prosecutors and regulators, refrain from all future criminal conduct, and implement remedial measures as required by its regulators. The $1.34 billion in penalties represents the second-largest penalty ever imposed on a financial institution for violations of U.S. economic sanctions.

From about 2004 to 2010, SG, in contravention of U.S. sanctions laws, operated 21 credit facilities that provided significant money flow to Cuban banks, entities controlled by Cuba, and Cuban and foreign corporations for business conducted in Cuba; those Cuban credit facilities involved substantial U.S.-cleared

payments through U.S. financial institutions in violation of the Trading with the Enemy Act and the Cuban Regulations. In total, SG engaged in more than 2,500 sanctions-violating transactions through U.S. financial institutions, causing it to process close to $13 billion in transactions that otherwise should have been rejected, blocked, or stopped for investigation pursuant to regulations promulgated by the Office of Foreign Assets Control. Most of these transactions and most of the total value involved a U.S. dollar credit facility designed to finance oil transactions between a Dutch commodities trading firm and a Cuban corporation with a state monopoly on producing and refining crude oil in Cuba.

SG avoided detection, in part, by making inaccurate or incomplete notations on payment messages that accompanied these sanctions-violating transactions. Indeed, the SG department that managed many of the Cuban credit facilities engaged in a deliberate practice of concealing the Cuban nexus of U.S. dollar payments that were made in connection with those facilities. For example, SG routed about 500 U.S. dollar–denominated payments through a particular Spanish bank to disguise the fact that the transactions violated U.S. sanctions, and employees were instructed to omit any references to Cuba or Cuban entities from the messages that accompanied the fund transfers.

Despite the awareness of both SG's senior management and Group Compliance that SG had engaged in this unlawful conduct, SG did not disclose its conduct to the Office of Foreign Assets Control or any other U.S. regulator, including the Board, or law enforcement agency until well after the government's investigation began.

This investigation was conducted by our office and the IRS–CI and prosecuted by the U.S. Attorney's Office for the Southern District of New York.

Former Acting President of CFG Community Bank Sentenced to Federal Prison for Bank Fraud and Tax Evasion

A former acting President of CFG Community Bank, a state member bank, was sentenced to 3 years in federal prison for bank fraud and tax evasion. The defendant was also ordered to pay $892,541.75 in restitution to CFG and $365,228.80 in restitution to the Internal Revenue Service and to forfeit $503,378.87.

According to court documents, the defendant diverted $100,000 in CFG funds for his own benefit while he was acting President. Later, while he was President of CFG affiliate Capital Financial Ventures, LLC, the defendant schemed to defraud CFG by posing as its current Chief Executive Officer and President to refinance CFG-owned mortgage loans. He then directed a settlement company to divert over $775,000 in loan proceeds for his personal benefit and the benefit of a friend. The defendant created false correspondence with the loan borrowers to conceal the diversion from CFG. The defendant also diverted

$91,126.56 in insurance premium refunds on one of the commercial loans purchased by CFG to his personal account instead of paying the funds over to the borrower.

In addition, in fall 2011 the defendant and codefendant attempted to realize a profit from a group of nonperforming mortgages their company, Capital T Partners Brookfield, LLC, had purchased by donating some of the mortgages to a charity and taking a charitable deduction on their income tax returns. The defendant admitted that he and the codefendant created a false Internal Revenue Service form 8283 and a false appraisal, which purported that the mortgages were valued at over $1 million. As a result, the defendant and codefendant received a valuable tax deduction. The defendant also admitted that he failed to report income of more than $176,000 in 2010 and $480,000 in 2011. The defendant underpaid his taxes for 2010, 2011, and 2012 by $365,228.80.

This was a joint investigation by our office, the FBI, the IRS–CI, and the Social Security Administration OIG and was prosecuted by the U.S. Attorney's Office for the District of Maryland.

Former Synovus Employee Pleaded Guilty to Bank Fraud and Tax Evasion

A former commercial banker for Synovus Bank, a state member bank, pleaded guilty to four counts of bank fraud and four counts of tax evasion.

Between July 2, 2013, and May 24, 2017, while managing some of the bank's largest clients, the defendant diverted $1,046,602 in client funds to a personal account at another bank. Financial records revealed that the defendant used these funds to pay for a wide assortment of his personal expenses, including payments on vehicles, credit card bills, vacations, jewelry, and cash withdrawals. In addition, the defendant failed to pay income taxes on the stolen money, amounting to $221,357.

This was a joint investigation by our office, the FBI, and the IRS–CI and was prosecuted by the U.S. Attorney's Office for the Middle District of Georgia.

Bureau of Consumer Financial Protection

Title X of the Dodd-Frank Act created the Bureau to implement and enforce federal consumer financial law. The Bureau's five statutory objectives are (1) to provide consumers with critical information about financial transactions, (2) to protect consumers from unfair practices, (3) to identify and address outdated and unduly burdensome regulations, (4) to foster transparency and efficiency in consumer financial product and service markets and to facilitate access and innovation, and (5) to enforce federal consumer financial law without regard to the status of the person to promote fair competition.

The Bureau supervises large banks, thrifts, and credit unions with total assets of more than $10 billion and certain nonbank entities, including mortgage brokers, loan modification providers, payday lenders, consumer reporting agencies, debt collectors, and private education lenders. Additionally, with certain exceptions, the Bureau's enforcement jurisdiction generally extends to individuals or entities that are engaging or have engaged in conduct that violates federal consumer financial law.

Our investigations concerning the Bureau's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the Bureau, lied to or misled examiners, or obstructed examinations in a manner that may have affected the Bureau's ability to carry out its supervisory responsibilities. Such activity may result in criminal violations, such as false statements or obstruction of examinations.

During this reporting period, no publicly reportable developments occurred in our ongoing investigations related to the Bureau.

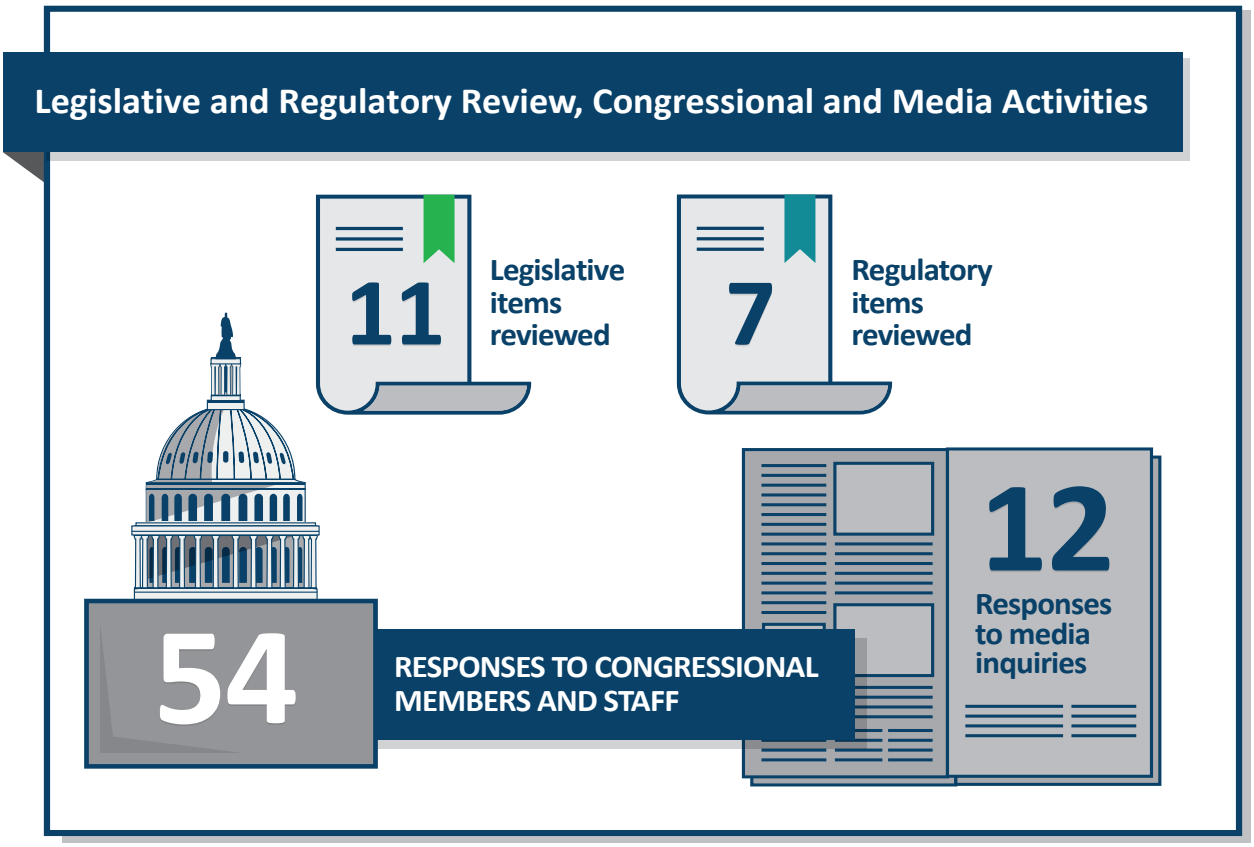
Hotline

The OIG Hotline helps people report fraud, waste, abuse, and mismanagement related to the programs or operations of the Board and the Bureau. Hotline staff can be reached by phone, web form, fax, or mail. We review all incoming hotline communications, research and analyze the issues raised, and determine how best to address the complaints.

During this reporting period, the OIG Hotline received 262 complaints. Complaints within the OIG's purview are evaluated and, when appropriate, referred to the relevant component within the OIG for audit, evaluation, investigation, or other review. Some complaints convey concerns about matters within the responsibility of other federal agencies or matters that should be addressed by a program or operation of the Board or the Bureau. The OIG Hotline refers such complaints to the appropriate federal agency for evaluation and resolution.

The OIG also continues to receive many noncriminal consumer complaints regarding consumer financial products and services. For these matters, the OIG Hotline typically refers complainants to the consumer group of the appropriate federal regulator for the institution involved, such as the Office of the Comptroller of the Currency's (OCC) Customer Assistance Group, the Bureau's Consumer Response team, or Federal Reserve Consumer Help.

Legislative and Regulatory Review, Congressional and Media Activities, and CIGIE Participation



Legislative and Regulatory Review

The Legal Services program is the independent legal counsel to the IG and OIG staff. Legal Services provides comprehensive legal advice, research, counseling, analysis, and representation in support of our audits, investigations, inspections, and evaluations as well as other professional, management, and administrative functions. Legal Services also keeps the IG and OIG staff aware of recent legal developments that may affect us, the Board, or the Bureau.

In accordance with section 4(a)(2) of the Inspector General Act of 1978, as amended, Legal Services independently reviews newly enacted and proposed legislation and regulations to determine their potential effect on the economy and efficiency of the Board's and the Bureau's programs and operations. During this reporting period, Legal Services reviewed 11 legislative items and 7 regulatory items.

Congressional and Media Activities

We communicate and coordinate with various congressional committees on issues of mutual interest. During this reporting period, we provided 54 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 12 media inquiries.

CIGIE Participation

The IG is a member of CIGIE, which provides a forum for IGs from various government agencies to discuss governmentwide issues and shared concerns. Collectively, CIGIE's members work to improve government programs and operations.

As part of the OIG community, we are proud to be part of the Oversight.gov effort. Oversight.gov is a searchable website containing the latest public reports from federal OIGs. It provides access to more than 11,000 reports, detailing for fiscal year 2018 alone over $32 billion in potential savings and over 7,000 recommendations to improve programs across the federal government.

The IG serves as a member of CIGIE's Legislation Committee, Investigations Committee, and Information Technology Committee. The Legislation Committee is the central point of information for legislative initiatives and congressional activities that may affect the OIG community, such as proposed cybersecurity legislation that was reviewed during the reporting period. The Investigations Committee advises the OIG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines. The Information Technology Committee facilitates effective IT audits, evaluations, and investigations and provides a forum for the expression of the OIG community's perspective on governmentwide IT operations.

Our Associate Inspector General for Information Technology, as the Chair of the Information Technology Committee of the Federal Audit Executive Council, works with IT audit staff throughout the OIG community and reports to the CIGIE Information Technology Committee on common IT audit issues.

Our Associate Inspector General for Legal Services and the Legal Services staff attorneys are members of the Council of Counsels to the Inspector General.

Peer Reviews

Government auditing and investigative standards require that our audit and investigative units be reviewed by a peer OIG organization every 3 years. The Inspector General Act of 1978, as amended, requires that OIGs provide in their semiannual reports to Congress information about (1) the most recent peer reviews of their respective organizations and (2) their peer reviews of other OIGs conducted within the semiannual reporting period. The following information addresses these requirements.

- In September 2017, the National Science Foundation OIG completed the latest peer review of our audit organization. We received a peer review rating of *pass*. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our audit organization.
- In April 2016, the Special Inspector General for Afghanistan Reconstruction completed the latest peer review of our Office of Investigations and rated us as compliant. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our investigations organization.

See our website for peer review reports of our organization.

Appendix A: Statistical Tables

Table A-1. Audit, Inspection, and Evaluation Reports Issued to the Board During the Reporting Period

Report title	Type of report
2018 Audit of the Board's Information Security Program	Audit
Evaluation of the Board's Implementation of Splunk	Evaluation
The Board Can Strengthen Information Technology Governance	Evaluation
The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration	Audit
The Board Can Strengthen Controls Over Its Academic Assistance Program	Audit
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2018 and 2017, and Independent Auditors' Reports	Audit
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2018 and 2017, and Independent Auditors' Reports	Audit
The Board Can Take Additional Steps to Advance Workforce Planning	Evaluation
Total number of audit reports: 5 Total number of evaluation reports: 3	

Table A-2. OIG Reports to the Board With Recommendations That Were Open During the Reporting Period

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
Response to a Congressional Request Regarding the Economic Analysis Associated with Specified Rulemakings	06/11	2	2	0	02/19	0	2
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	0	03/19	7	1
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	0	01/19	0	1
Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	07/14	3[a]	3	0	02/19	2	1
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle	12/14	3	3	0	10/18	2	1
Review of the Failure of Waccamaw Bank	03/15	5	5	0	03/19	3	2
Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)	09/15	3	3	0	03/19	0	3

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations	04/16	9	9	0	03/19	9	0
Security Control Review of the Board's Active Directory Implementation (nonpublic report)	05/16	10	10	0	03/19	1	9
2016 Audit of the Board's Information Security Program	11/16	9	9	0	10/18	7	2
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	0	03/19	7	4
The Board Can Improve Documentation of Office of Foreign Assets Control Examinations	03/17	2	2	0	03/19	2	0
The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool	03/17	2	2	0	03/19	2	0
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing	04/17	8	8	0	02/19	4	4
2017 Audit of the Board's Information Security Program	10/17	9	9	0	10/18	2	7

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	03/19	3	11
Security Control Review of the RADAR Data Warehouse (nonpublic report)	03/18	3	3	0	n.a.	0	3
Review of the Failure of Allied Bank	03/18	2	2	0	03/19	2	0
Security Control Review of the Board's Public Website (nonpublic report)	03/18	7	7	0	03/19	0	7
In Accordance With Applicable Guidance, Reserve Banks Rely on the Primary Federal Regulator of the Insured Depository Institution in the Consolidated Supervision of Regional Banking Organizations, but Document Sharing Can Be Improved	06/18	3	3	0	03/19	3	0
Knowledge Management for the Board's Comprehensive Liquidity Analysis and Review Is Generally Effective and Can Be Further Enhanced	09/18	3	3	0	n.a.	1	2
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic report)	09/18	9	9	0	n.a.	0	9
2018 Audit of the Board's Information Security Program	10/18	6	6	0	n.a.	0	6

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
Evaluation of the Board's Implementation of Splunk (nonpublic report)	11/18	1	1	0	n.a.	0	1
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	n.a.	1	5
The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration	12/18	8	8	0	n.a.	0	8
The Board Can Strengthen Controls Over Its Academic Assistance Program	12/18	9	9	0	n.a.	0	9
The Board Can Take Additional Steps to Advance Workforce Planning	03/19	2	2	0	n.a.	0	2

Note. A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable; or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the agency is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation and we have referred or are referring it to the appropriate oversight committee or administrator for a final decision.

n.a. not applicable.

a. These recommendations were directed jointly to the OCC, the FDIC, and the Board.

Table A-3. Audit, Inspection, and Evaluation Reports Issued to the Bureau During the Reporting Period

Report title	Type of report
2018 Audit of the Bureau's Information Security Program	Audit
Bureau Purchase Card Program Controls Appear to Be Operating Effectively	Audit
The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions	Evaluation
The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities	Evaluation
Total number of audit reports: 2 Total number of evaluation reports: 2	

Table A-4. OIG Reports to the Bureau With Recommendations That Were Open During the Reporting Period

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity	09/13	14	14	0	03/19	13	1
Security Control Review of the CFPB's Cloud Computing–Based General Support System (nonpublic report)	07/14	4	4	0	03/19	4	0
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	10/18	2	1
The CFPB Can Enhance Its Diversity and Inclusion Efforts	03/15	17	17	0	03/18	16	1
The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	0	03/19	6	3
2016 Audit of the CFPB's Information Security Program	11/16	3	3	0	10/18	2	1
The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information	05/17	9	9	0	12/18	9	0
Security Control Review of the CFPB's Public Website (nonpublic report)	05/17	8	8	0	12/18	8	0

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The CFPB Can Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-Job Training Program	09/17	9	9	0	03/19	9	0
The CFPB Can Improve Its Examination Workpaper Documentation Practices	09/17	17	17	0	01/19	3	14
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	01/19	4	3
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	11/18	4	7
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	n.a.	0	2
The Bureau Could Have Better Managed Its GMMB Contract and Should Strengthen Controls for Contract Financing and Contract Management	06/18	7	7	0	10/18	7	0
Security Control Review of the Bureau's Mosaic System (nonpublic report)	06/18	1	1	0	01/19	1	0
The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened	09/18	4	4	0	03/19	0	4

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	n.a.	0	4
The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions	01/19	6	6	0	n.a.	0	6
The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities	03/19	4	4	0	n.a.	1	3

Note. A recommendation is closed if (1) the corrective action has been taken; (2) the recommendation is no longer applicable; or (3) the appropriate oversight committee or administrator has determined, after reviewing the position of the OIG and division management, that no further action by the agency is warranted. A recommendation is open if (1) division management agrees with the recommendation and is in the process of taking corrective action or (2) division management disagrees with the recommendation and we have referred or are referring it to the appropriate oversight committee or administrator for a final decision.

n.a. not applicable.

Table A-5. Audit, Inspection, and Evaluation Reports Issued to the Board and the Bureau With Questioned Costs, Unsupported Costs, or Recommendations That Funds Be Put to Better Use During the Reporting Period

Reports	Number	Dollar value
With questioned costs, unsupported costs, or recommendations that funds be put to better use, regardless of whether a management decision had been made	0	$0

Note. Because the Board and the Bureau are primarily regulatory and policymaking agencies, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable. In the event that an audit, inspection, or evaluation report contains quantifiable information regarding questioned costs, unsupported costs, or recommendations that funds be put to better use, this table will be expanded.

Table A-6. Summary Statistics on Investigations During the Reporting Period

Investigative actions	Number or dollar value[a]
Investigative caseload	
Investigations open at end of previous reporting period	56
Investigations opened during the reporting period	19
Investigations closed during the reporting period	13
Investigations open at end of the reporting period	62
Investigative results for the reporting period	
Persons referred to U.S. Department of Justice prosecutors	10
Persons referred to state/local prosecutors	0
Declinations received	6
Joint investigations	37
Reports of investigation issued	0
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	0
Suspensions	0
Debarments	0
Prohibitions from banking industry	1
Indictments	0
Criminal informations	2
Criminal complaints	1

See notes at end of table.

Investigative actions	Number or dollar value[a]
Convictions	2
Civil actions	$0
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$0
Criminal fines, restitution, and special assessments	$1,340,901,300
Forfeiture	$0

Note. Some of the investigative numbers may include data also captured by other OIGs.

a. Metrics: These statistics were compiled from the OIG's investigative case management and tracking system.

Table A-7. Summary Statistics on Hotline Activities During the Reporting Period

Hotline complaints	Number
Complaints pending from previous reporting period	27
Complaints received during reporting period	262
Total complaints for reporting period	289
Complaints resolved during reporting period	274
Complaints pending	15

Appendix B: Inspector General Empowerment Act of 2016 Requirements

The Inspector General Empowerment Act of 2016 amended section 5 of the Inspector General Act of 1978 by adding reporting requirements that must be included in OIG semiannual reports to Congress. These additional reporting requirements include summaries of certain audits, inspections, and evaluations; investigative statistics; summaries of investigations of senior government employees; whistleblower retaliation statistics; summaries of interference with OIG independence; and summaries of closed audits, evaluations, inspections, and investigations that were not publicly disclosed. Our response to these requirements is below.

Summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which no agency comment was returned within 60 days of receiving the report or for which no management decision has been made by the end of the reporting period.

- We have no such instances to report.

Summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.

- See appendix C.

Statistical tables showing for the reporting period (1) the number of issued investigative reports, (2) the number of persons referred to the U.S. Department of Justice for criminal prosecution, (3) the number of persons referred to state and local authorities for criminal prosecution, and (4) the number of indictments and criminal informations that resulted from any prior referral to prosecuting authorities. Describe the metrics used to develop the data for these new statistical tables.

- See table A-6.

A report on each investigation conducted by the OIG that involves a senior government employee in which allegations of misconduct were substantiated, which includes (1) a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter, (2) whether the matter was referred to the U.S. Department of Justice and the date of the referral, and (3) whether the U.S. Department of Justice declined the referral and the date of such declination.

- We initiated an investigation concerning allegations that a Board employee engaged in inappropriate conduct while on government time and during government travel. The investigation substantiated the allegations and determined that the employee used their Board-issued IT equipment inappropriately and knowingly violated IT policy. We presented this matter to the U.S. Department of Justice, which declined prosecution on October 10, 2018. The employee subsequently resigned. This investigation was closed.

A detailed description of any instance of whistleblower retaliation, including information about the official found to have engaged in retaliation and what, if any, consequences the agency imposed to hold that official accountable.

- We have no such instances to report.

A detailed description of any attempt by the Board or the Bureau to interfere with the independence of the OIG, including (1) through budget constraints designed to limit OIG capabilities and (2) incidents when the agency has resisted or objected to OIG oversight activities or restricted or significantly delayed OIG access to information, including the justification of the establishment for such action.

- We have no such attempts to report.

Detailed descriptions of (1) inspections, evaluations, and audits conducted by the OIG that were closed and not disclosed to the public and (2) investigations conducted by the OIG involving a senior government employee that were closed and not disclosed to the public.

- We have no such instances to report.

Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations

The Inspector General Empowerment Act of 2016 requires that we provide summaries of each audit, inspection, and evaluation report issued to the Board or the Bureau for which there are outstanding unimplemented recommendations, including the aggregate potential cost savings of those recommendations.

Board of Governors of the Federal Reserve System

Table C-1. Reports to the Board With Unimplemented Recommendations, by Calendar Year

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2011	1	2
2012	1	1
2013	1	1
2014	2	2
2015	2	5
2016	3	15
2017	3	22
2018	9	50
2019[a]	1	2

Note. Because the Board is primarily a regulatory and policymaking agency, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable.

a. Through March 31, 2019.

Response to a Congressional Request Regarding the Economic Analysis Associated with Specified Rulemakings

June 13, 2011

Total number of recommendations: 2
Recommendations open: 2

In May 2011, we received a letter from the minority members of the Senate Committee on Banking, Housing, and Urban Affairs requesting that we review the economic analysis that the Board performed supporting five Dodd-Frank Act rulemakings.

We found that the Board routinely reviewed economic data to monitor changing economic conditions and conducted the quantitative economic analysis necessary to satisfy statutory requirements and, on a discretionary basis, to support the rulemaking. Further, we determined that the Board generally sought public input for its rulemaking activities and typically reevaluates the effectiveness of its existing regulations every 5 years. We concluded that the Board generally followed a similar approach for the five rulemakings we reviewed and that those rulemakings complied with the Paperwork Reduction Act, the Regulatory Flexibility Act, and applicable Dodd-Frank Act requirements described in our report.

Our analysis yielded the following findings that resulted in recommendations. First, the Board's policy statement on rulemaking procedures had not been recently updated and, although rulemaking staff were cognizant of the Board's rulemaking practices, none of the staff members cited the policy statement. Second, our review of the *Federal Register* indicated that the notices associated with the respective rulemakings typically provided insight into the general approaches and data used in the economic analysis; however, in some cases, the Board's internal documentation did not clearly outline the work steps underlying the economic analysis.

Security Control Review of the National Remote Access Services System (nonpublic report)

March 30, 2012

Total number of recommendations: 8
Recommendations open: 1

We completed a security control review of the Federal Reserve System's National Remote Access Services (NRAS) system. The Board and the 12 Reserve Banks use NRAS to remotely access Board and Reserve Bank information systems. Our objectives were to evaluate the effectiveness of selected security controls and techniques to ensure that the Board maintains a remote access program that is generally compliant with FISMA requirements.

Overall, our review found that NRAS was technically and operationally sound and that the Board had developed an adequate process to administer token keys for Board personnel. However, we identified opportunities to strengthen information security controls to help ensure that NRAS meets FISMA requirements.

The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control

2013-AE-B-013 **September 5, 2013**

Total number of recommendations: 1
Recommendations open: 1

Our objective for this audit was to determine the processes for establishing, maintaining, and monitoring internal control within the Board.

We found that the Board's divisions had processes for establishing administrative internal control that were tailored to their specific responsibilities. These controls generally used best practices and were designed to increase efficiency and react to changing environments; however, the Board's processes for maintaining and monitoring these controls could have been enhanced. Specifically, we found that the Board did not have an agencywide process for maintaining and monitoring its administrative internal control. An agencywide process that maintains, monitors, and reports on administrative internal control can assist the Board in effectively and efficiently achieving its mission, goals, and objectives, as well as address the organizational challenges outlined in the Board's 2012–2015 strategic framework.

Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions

2014-SR-B-011 **July 25, 2014**

Total number of recommendations: 3[4]
Recommendations open: 1

Our office, the FDIC OIG, and the Treasury OIG participated in this evaluation concerning actions that the FDIC, the Board, and the OCC took against individuals and entities in response to actions that harmed financial institutions. The objectives of the evaluation were (1) to describe the FDIC's, the Board's, and the OCC's processes for investigating and pursuing enforcement actions against institution-affiliated parties associated with failed institutions, as well as the results of those efforts; (2) to describe the FDIC's process for investigating and pursuing professional liability claims against individuals and entities associated

4. Two of these recommendations were directed jointly to the Board, the OCC, and the FDIC. One recommendation was directed to the Board and the OCC.

with failed institutions and its coordination with the Board and the OCC; (3) to determine the results of the FDIC's, the Board's, and the OCC's efforts in investigating and pursuing enforcement actions against institution-affiliated parties and the FDIC's efforts in pursuing professional liability claims; and (4) to assess key factors that may impact the pursuit of enforcement actions and professional liability claims.

The joint evaluation team found that several factors appeared to affect the three regulators' ability to pursue enforcement actions against institution-affiliated parties. Those factors included the rigorous statutory criteria for sustaining removal/prohibition orders; the extent to which each regulator was willing to use certain enforcement action tools, such as personal cease-and-desist orders; the risk appetite of the FDIC, the Board, and the OCC for bringing enforcement actions; enforcement action statutes of limitation; and staff resources. We also noted opportunities for these regulators to address differences in how they notify each other when initiating enforcement actions against institution-affiliated parties and depository institutions.

Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle

2014-IT-B-021 **December 18, 2014**

Total number of recommendations: 3
Recommendations open: 1

We performed this audit of the operational efficiency and effectiveness of the Board's information security life cycle pursuant to requirements set forth in FISMA.

Overall, we found that the Chief Information Officer maintained a FISMA-compliant information security program that was consistent with requirements for certification and accreditation established by the National Institute of Standards and Technology and the Office of Management and Budget. However, we identified opportunities to improve the operational efficiency and effectiveness of the Board's management of its information security life cycle.

Review of the Failure of Waccamaw Bank

2015-SR-B-005 **March 26, 2015**

Total number of recommendations: 5
Recommendations open: 2

In accordance with Dodd-Frank Act requirements, we concluded that Waccamaw Bank's failure presented unusual circumstances that warranted an in-depth review. Based on the in-depth review, we determined that Waccamaw Bank failed because its board of directors and senior management did not control the risks associated with the bank's rapid growth strategy. As a result, the bank sustained significant losses

during a downturn in its local real estate market. In addition, we learned that (1) supervisory activity records were not retained in accordance with Board policy, (2) Waccamaw Bank's written agreement did not contain a provision that required regulatory approval of material transactions, and (3) Board and Federal Reserve Bank of Richmond appeals policies were silent on procedural aspects for second-level and third-level appeals.

Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)

2015-IT-B-015 **September 2, 2015**

Total number of recommendations: 3
Recommendations open: 3

We completed a security control review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (C-SCAPE). Our audit objective was to evaluate the adequacy of selected security controls implemented by the Board to protect C-SCAPE from unauthorized access, modification, destruction, and disclosure. We also evaluated C-SCAPE's compliance with FISMA and the information security policies, procedures, standards, and guidelines of the Board.

Overall, we found that the Board had taken steps to secure the C-SCAPE application in accordance with FISMA and the Board's information security program. However, during vulnerability scanning of the databases supporting C-SCAPE, we found vulnerabilities that required the attention of the C-SCAPE application owner and the Board's Division of Information Technology. Additionally, we noted that the C-SCAPE application audit logs did not record certain database activity on financial institution information.

Security Control Review of the Board's Active Directory Implementation (nonpublic report)

2016-IT-B-008 **May 11, 2016**

Total number of recommendations: 10
Recommendations open: 9

As required by FISMA, we evaluated the administration and security design effectiveness of the Active Directory operating environment implemented at the Board. To accomplish this objective, we determined whether (1) the Board had conducted a proper risk assessment of the Active Directory domain; (2) tools and processes had been implemented to continuously monitor the Active Directory domain; (3) these tools and processes allowed for users (active employees, contractors, super users, administrators, and others) to be properly identified; (4) the Active Directory domain was properly configured and scanned for vulnerabilities; and (5) contingency planning processes had been established for the Active Directory domain.

Overall, we found that the Board was effectively administering and protecting the Active Directory infrastructure. We found, however, that the Board could have strengthened Active Directory controls in the areas of risk management, continuous monitoring, user group management, contractor account management, and system documentation. In addition, we identified a risk for management's continued attention related to transport layer security.

2016 Audit of the Board's Information Security Program

2016-IT-B-013 **November 10, 2016**

Total number of recommendations: 9
Recommendations open: 2

In accordance with FISMA requirements, we reviewed the Board's information security program. Specifically, we evaluated the effectiveness of the Board's (1) security controls and techniques and (2) information security policies, procedures, and practices.

We found that the Board had taken several steps to mature its information security program to ensure that the program was consistent with FISMA requirements. For instance, we found that the Board had implemented an enterprisewide information security continuous monitoring lessons-learned process as well as strengthened its system-level vulnerability management practices. However, we identified several improvements needed in the Board's information security program in the areas of risk management, identity and access management, security and privacy training, and incident response. Specifically, we found that the Board could have strengthened its risk management program by ensuring that Board divisions were consistently implementing the organization's risk management processes related to security controls assessment, security planning, and authorization. In addition, we found instances of Board sensitive information that was not appropriately restricted within the organization's enterprisewide collaboration tool. We also noted that the Board had not evaluated the effectiveness of its security and privacy awareness training program in 2016. Finally, we found that the Board could have strengthened its incident response capabilities.

Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities

2016-SR-B-014 **November 14, 2016**

Total number of recommendations: 11
Recommendations open: 4

We initiated this evaluation in response to a written request from the Director of the Board's Division of Banking Supervision and Regulation[5] and the Board's General Counsel. Our objectives were (1) to assess the methods for Federal Reserve System decisionmakers to obtain material information necessary to ensure that decisions and conclusions resulting from supervisory activities at Large Institution Supervision Coordinating Committee firms and large banking organizations were appropriate, supported by the record, and consistent with applicable policies and (2) to determine whether there were adequate channels for System decisionmakers to be aware of supervision employees' divergent views about material issues regarding Large Institution Supervision Coordinating Committee firms and large banking organizations.

We found that employees' willingness to share views varied by Reserve Bank and among supervision teams at the same Reserve Bank. We also found that leadership and management approaches played a major role in influencing employees' comfort level with sharing views. We identified five root causes for employees' reticence to share their views. In addition, we described several leadership behaviors and processes employed by the leadership at certain Reserve Banks that appeared particularly effective in convincing Reserve Bank supervision employees that sharing their views was both safe and worthwhile.

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**

Total number of recommendations: 8
Recommendations open: 4

We assessed (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. We found that the Division of Supervision and Regulation could improve the oversight of MDPS firms by (1) enforcing a reporting requirement in the Bank Service Company Act, (2) considering the implementation of an enhanced governance structure for these firms,

5. The Division of Banking Supervision and Regulation is now the Division of Supervision and Regulation.

(3) providing additional guidance on the supervisory expectations for these firms, and (4) ensuring that the division's intelligence and incident management function is aware of the technologies used by MDPS firms. We also identified opportunities to improve the recruiting, retention, tracking, and succession planning of cybersecurity resources, as well as opportunities to enhance the internal communications about cybersecurity-related risks.

2017 Audit of the Board's Information Security Program

2017-IT-B-018 **October 31, 2017**

Total number of recommendations: 9
Recommendations open: 7

We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

The Board's information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. Further, it has implemented an effective security training program that includes phishing exercises and associated performance metrics. However, the Board can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). The lack of an agencywide risk-management governance structure and strategy as well as decentralized IT services result in an incomplete view of the risks affecting the security posture of the Board and impede its ability to implement an effective information security program. In addition, several security processes, such as configuration management and information security continuous monitoring, were not effectively implemented agencywide.

The Board's Organizational Governance System Can Be Strengthened

2017-FMIC-B-020 **December 11, 2017**

Total number of recommendations: 14
Recommendations open: 11

An organization's governance system determines how decisionmaking, accountability, controls, and behaviors help accomplish its objectives. Our evaluation (1) describes the current state of the Board's organizational governance structures and processes and (2) assesses the extent to which these structures and processes align with those of other relevant institutions and with governance principles.

The Board's core organizational governance structure aligns with benchmark institutions and selected governance principles, as does its public disclosure of governance documents. Nonetheless, the Board can strengthen its governance system by clarifying and regularly reviewing purposes, roles and responsibilities, authorities, and working procedures of its standing committees; enhancing the orientation program for new Governors and reviewing and formalizing the process for selecting dedicated advisors; setting clearer communication expectations and exploring additional opportunities for information sharing among Governors; reviewing, communicating, and reinforcing the Board of Governors' expectations of the Chief Operating Officer and the heads of the administrative functions; and establishing and documenting the Executive Committee's mission, protocols, and authorities.

Security Control Review of the RADAR Data Warehouse (nonpublic report)

2018-IT-B-006R **March 7, 2018**

Total number of recommendations: 3
Recommendations open: 3

We assessed the effectiveness of select security controls for the Risk Assessment, Data Analysis, and Research (RADAR) Data Warehouse and associated query tools. The RADAR Data Warehouse gives Federal Reserve System and Board staff access to mortgage and consumer data for supervision and research purposes. It has been classified as a moderate-risk system.

Overall, the information security controls that we tested were operating effectively. However, controls in the areas of contingency planning, configuration management, and security assessment and authorization can be strengthened.

Security Control Review of the Board's Public Website (nonpublic report)

2018-IT-B-008R **March 21, 2018**

Total number of recommendations: 7
Recommendations open: 7

We evaluated the adequacy of select information security controls for protecting the Board's public website from compromise. Overall, the information security controls that we tested were adequately designed and implemented. However, we identified opportunities for improvement in the areas of configuration management and risk management.

Knowledge Management for the Board's Comprehensive Liquidity Analysis and Review Is Generally Effective and Can Be Further Enhanced

2018-SR-B-013 **September 5, 2018**

Total number of recommendations: 3
Recommendations open: 2

We assessed the System's knowledge management processes, practices, and systems in support of the Comprehensive Liquidity Analysis and Review (CLAR) program.

The CLAR program appears to preserve and maintain institutional knowledge related to supervisory findings and fosters effective collaboration; however, knowledge management practices can be further strengthened by (1) increasing CLAR program employees' awareness of management's office hours, during which they can discuss the rationale for decisions made during the CLAR letter-writing process; (2) formalizing employee onboarding procedures; and (3) standardizing the CLAR Steering Committee's approach to meeting minutes.

Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic report)

2018-IT-B-015R **September 26, 2018**

Total number of recommendations: 9
Recommendations open: 9

We evaluated the effectiveness of select security controls and techniques for the Division of Research and Statistics' general support system, as well as the system's compliance with FISMA and Board information security policies, procedures, standards, and guidelines.

Overall, we found that the division has taken steps to implement information security controls for its general support system in accordance with FISMA and Board information security policies, procedures, standards, and guidelines. We identified opportunities for improvement in the implementation of the Board's information system security life cycle for the division's general support system to ensure that information security controls are effectively implemented, assessed, authorized, and monitored.

2018 Audit of the Board's Information Security Program

2018-IT-B-017 **October 31, 2018**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

Evaluation of the Board's Implementation of Splunk (nonpublic report)

2018-IT-B-019R **November 5, 2018**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

The Board Can Strengthen Information Technology Governance

2018-IT-B-020 **November 5, 2018**

Total number of recommendations: 6
Recommendations open: 5

See the summary in the body of this report.

The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration

2018-FMIC-B-021 **December 3, 2018**

Total number of recommendations: 8
Recommendations open: 8

See the summary in the body of this report.

The Board Can Strengthen Controls Over Its Academic Assistance Program

2018-MO-B-023 **December 12, 2018**

Total number of recommendations: 9
Recommendations open: 9

See the summary in the body of this report.

The Board Can Take Additional Steps to Advance Workforce Planning

2019-MO-B-004 **March 25, 2019**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

Bureau of Consumer Financial Protection

Table C-2. Reports to the Bureau With Unimplemented Recommendations, by Calendar Year

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2013	1	1
2014	1	1
2015	1	1
2016	2	4
2017	2	17
2018	4	17
2019[a]	2	9

Note. Because the Bureau is primarily a regulatory and policymaking agency, our recommendations typically focus on program effectiveness and efficiency, as well as strengthening internal controls. As such, the monetary benefit associated with their implementation typically is not readily quantifiable.

a. Through March 31, 2019.

The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity

2013-AE-C-017 **September 30, 2013**

Total number of recommendations: 14
Recommendations open: 1

We determined the effectiveness of the Bureau's internal controls for its government travel card (GTC) program.

We found opportunities to strengthen internal controls to ensure program integrity. Although controls over the card issuance process were designed and operating effectively, controls were not designed or operating effectively (1) to prevent and detect fraudulent or unauthorized use of cards and (2) to provide reasonable assurance that cards were properly monitored and closed out.

2014 Audit of the CFPB's Information Security Program

2014-IT-C-020 **November 14, 2014**

Total number of recommendations: 3
Recommendations open: 1

We found that the Bureau continued to take steps to mature its information security program and to ensure that it was consistent with the requirements of FISMA. Overall, we found that the Bureau's information security program was consistent with 9 of 11 information security areas. Although corrective actions were underway, further improvements were needed in security training and contingency planning. We found that the Bureau's information security program was generally consistent with the requirements for continuous monitoring, configuration management, and incident response; however, we identified opportunities to strengthen these areas through automation and centralization.

The CFPB Can Enhance Its Diversity and Inclusion Efforts

2015-MO-C-002 **March 4, 2015**

Total number of recommendations: 17
Recommendations open: 1

Our review of the Bureau's diversity and inclusion efforts was conducted in response to a congressional request. Overall, our audit determined that the Bureau had taken steps to foster a diverse and inclusive workforce since it began operations in July 2011.

We identified four areas of the Bureau's diversity and inclusion efforts that could be enhanced. First, diversity and inclusion training was not mandatory for Bureau employees, supervisors, and senior managers. Second, data quality issues existed in the Bureau's tracking spreadsheets for equal employment opportunity complaints and negotiated grievances, and certain data related to performance management were not analyzed for trends that could indicate potential diversity and inclusion issues. Third, the Bureau's diversity and inclusion strategic plan had not been finalized, and opportunities existed for the Bureau to strengthen supervisors' and senior managers' accountability for implementing diversity and inclusion initiatives and human resources–related policies. Finally, the Bureau could have benefited from a formal succession planning process to help ensure a sufficient and diverse pool of candidates for its senior management positions.

The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program

2016-FMIC-C-009 **June 27, 2016**

Total number of recommendations: 9
Recommendations open: 3

Our objective was to determine whether the Bureau had established and maintained internal controls for its GTC program in accordance with the Government Charge Card Abuse Prevention Act of 2012.

We found that although the Bureau had implemented several controls over its program, some controls were not designed or operating effectively (1) to prevent or identify unauthorized use of cards and (2) to provide reasonable assurance that cards were closed in a timely manner upon employees' separation.

2016 Audit of the CFPB's Information Security Program

2016-IT-C-012 **November 10, 2016**

Total number of recommendations: 3
Recommendations open: 1

In accordance with FISMA requirements, we reviewed the Bureau's information security program. Our audit objectives were to evaluate the effectiveness of the Bureau's (1) security controls and techniques and (2) information security policies, procedures, and practices.

We found that the Bureau had taken several steps to mature its information security program to ensure that it was consistent with FISMA requirements. For instance, we found that both the information security continuous monitoring and incident response programs were operating at an overall maturity of level 3 (*consistently implemented*). However, we identified several improvements needed in the Bureau's information security program in the areas of risk management, identity and access management, and contingency planning. Specifically, we noted that the Bureau could have strengthened its risk management program by formalizing its insider threat activities and evaluating options to develop an agencywide insider threat program that leverages planned activities around data loss prevention. Related to the management of insider threat risks, signed rules of behavior documents were not in place for several privileged users who were not consistently resubmitting user access forms to validate the need for their elevated access. We also noted that the Bureau had not completed an agencywide business impact analysis to guide its contingency planning activities, nor had it fully updated its continuity of operations plan to reflect the transition of its IT infrastructure from Treasury.

The CFPB Can Improve Its Examination Workpaper Documentation Practices

2017-SR-C-016 **September 27, 2017**

Total number of recommendations: 17
Recommendations open: 14

We reviewed workpaper documentation in each of the Bureau's four regions for compliance with the *CFPB Supervision and Examination Manual* and other policies that govern examination work.

We found that, subject to certain conditions being met, SEFL's approach was to grant examination employees in each region open access to all examination workpaper documentation and supporting materials. This approach resulted in certain division employees having access to materials with confidential supervisory information and personally identifiable information when they did not appear to have a business need to know that information.

We also found opportunities to reinforce the need to store workpapers in the appropriate location and to document supervisory reviews and sampling methods.

2017 Audit of the CFPB's Information Security Program

2017-IT-C-019 **October 31, 2017**

Total number of recommendations: 7
Recommendations open: 3

We evaluated the effectiveness of the Bureau's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

The Bureau's overall information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. However, the Bureau can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). Specifically, the agency can strengthen its ongoing efforts to establish an enterprise risk-management program by defining a risk appetite statement and associated risk tolerance levels and developing and maintaining an agencywide risk profile. It can also improve configuration monitoring processes for agency databases and applications, multifactor authentication for the internal network and systems, assessments of the effectiveness of security awareness and training activities, and incident response and contingency planning capabilities.

The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data

2018-MO-C-001 **January 22, 2018**

Total number of recommendations: 11
Recommendations open: 7

The Bureau's offboarding process for employees and contractors covers, among other things, the return of property, records management, and ethics counseling on conflicts of interest. We determined whether the agency's controls over these aspects of offboarding effectively mitigate reputational and security risks.

Although the Bureau has offboarding controls related to conflicts of interest for executive employees' postemployment restrictions, the Bureau has opportunities to strengthen controls in other areas. Specifically, the agency did not always deactivate badges timely or record the status of badges for separating employees and contractors, did not consistently maintain IT asset documentation, did not always conduct records briefings, did not always maintain nondisclosure agreements for contractors, and did not accurately maintain certain separation and contractor data.

Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program

2018-IT-C-003 **February 14, 2018**

Total number of recommendations: 2
Recommendations open: 2

We contracted with a third party to conduct a performance audit of the Bureau's privacy program and its implementation.

Overall, the contractor found that the Bureau has substantially developed, documented, and implemented a privacy program that addresses applicable federal privacy requirements and security risks related to collecting, processing, handling, storing, and disseminating sensitive privacy data. Further, the contractor noted that the Bureau has documented privacy policies and procedures covering a wide range of topics, including privacy roles and responsibilities, privacy impact assessment and system of records notice management, training, breach notification and response, and monitoring and auditing.

The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened

2018-FMIC-C-014 **September 26, 2018**

Total number of recommendations: 4
Recommendations open: 4

Our objective was to determine whether the Bureau's GTC program controls are effectively designed and operating to prevent or identify instances of illegal, improper, or erroneous travel expenses and payments.

Although the Bureau's GTC controls are generally effective, they could be further strengthened to prevent improper reimbursements. In a few cases, cardholders received duplicative reimbursements for multicity trips. In others, they received reimbursements for unallowable expenses incurred during leave while on official travel. In addition, the Bureau has enhanced controls to ensure compliance with *Federal Travel Regulation* requirements related to reimbursing official travel expenses for traveling by personally owned vehicle, but it should strengthen controls to ensure compliance with requirements related to excess time spent traveling by personally owned vehicle.

2018 Audit of the Bureau's Information Security Program

2018-IT-C-018 **October 31, 2018**

Total number of recommendations: 4
Recommendations open: 4

See the summary in the body of this report.

The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions

2019-SR-C-001 **January 28, 2019**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities

2019-SR-C-005 **March 25, 2019**

Total number of recommendations: 4
Recommendations open: 3

See the summary in the body of this report.

Abbreviations

Board	Board of Governors of the Federal Reserve System
Bureau	Bureau of Consumer Financial Protection
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CLAR	Comprehensive Liquidity Analysis and Review
C-SCAPE	Consolidated Supervision Comparative Analysis, Planning and Execution System
DATA Act	Digital Accountability and Transparency Act of 2014
DIF	Deposit Insurance Fund
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
GTC	government travel card
IG	Inspector General
IPIA	Improper Payments Information Act of 2002, as amended
IRS–CI	Internal Revenue Service–Criminal Investigation
IT	information technology
MDPS	multiregional data processing servicer
MRAs	Matters Requiring Attention
NRAS	National Remote Access Services
OCC	Office of the Comptroller of the Currency
OIG	Office of Inspector General
RADAR	Risk Assessment, Data Analysis, and Research
SEC	U.S. Securities and Exchange Commission
SEFL	Division of Supervision, Enforcement and Fair Lending

SG	Société Générale S.A.
Treasury	U.S. Department of the Treasury

Office of Inspector General

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

20th Street and Constitution Avenue NW
Mail Stop K-300
Washington, DC 20551
Phone: 202-973-5000 | Fax: 202-973-5044

OIG Hotline

oig.federalreserve.gov/hotline
oig.consumerfinance.gov/hotline

800-827-3340