Office of Inspector General

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

Semiannual Report to Congress

April 1, 2018–September 30, 2018

OIG

Semiannual Report to Congress

April 1, 2018–September 30, 2018

Office of Inspector General

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

Message From the Inspector General

This year marks the 40th anniversary of the Inspector General Act of 1978, which established the first 12 Inspectors General in federal departments and agencies. The act, which passed by large margins and with bipartisan support, empowered the Inspectors General to curb waste, fraud, and abuse and to promote economy and efficiency in government operations. While the Inspector General community has grown larger over the past 40 years, it has remained fundamentally committed to overseeing and improving the programs and operations of federal government.

During the past 6 months, we issued four reports related to the Board of Governors of the Federal Reserve System's (Board) programs. These reports addressed the Federal Reserve Banks' reliance on consolidated supervision of regional banking organizations; knowledge management practices supporting the supervision of large, complex financial firms; information security controls for the Division of Research and Statistics; and the failure of Fayette County Bank. We issued four reports on the Bureau of Consumer Financial Protection's (Bureau) operations, which covered the Civil Penalty Fund's compliance with the Improper Payments Information Act of 2002, as amended; contract financing for and management of the GMMB contract; a security control review of the Mosaic application used to manage consumer complaints; and a review of travel card program controls.

We also provided the agencies with independent investigative oversight. Our Office of Investigations pursued bank fraud, obstruction, bribery of a public official, and other cases related to the programs and operations of the Board and the Bureau. We processed 272 new hotline complaints and closed 15 investigations. Our work resulted in 9 persons referred for criminal prosecution; 4 indictments; and over $2.5 million in civil judgments, criminal fines, restitution, and special assessments. Our investigative work continues to demonstrate that those who commit wrongdoing against the Board or the Bureau will be held accountable.

We have continued to engage with stakeholders inside and outside the Board and the Bureau. We remain an active presence with current Board, Bureau, and Reserve Bank senior leadership, and we look forward to working with the new Board Vice Chairman. Since our previous report, we have met with five key members of our oversight committees. Finally, we have continued to connect with the public through outreach and through Oversight.gov, a publicly accessible, searchable website that contains the latest public reports from Inspectors General.

President Jimmy Carter described the newly established Inspectors General as "perhaps the most important new tools in the fight against fraud." As we commemorate the 40th anniversary of the Inspector General Act, the role of independent oversight remains as critical as ever. I am proud that our work is making a positive difference. Of course, we could not fulfill our mission without our talented and dedicated staff. I am deeply grateful to the OIG staff for their exemplary work and steadfast commitment to our mission, vision, and values.

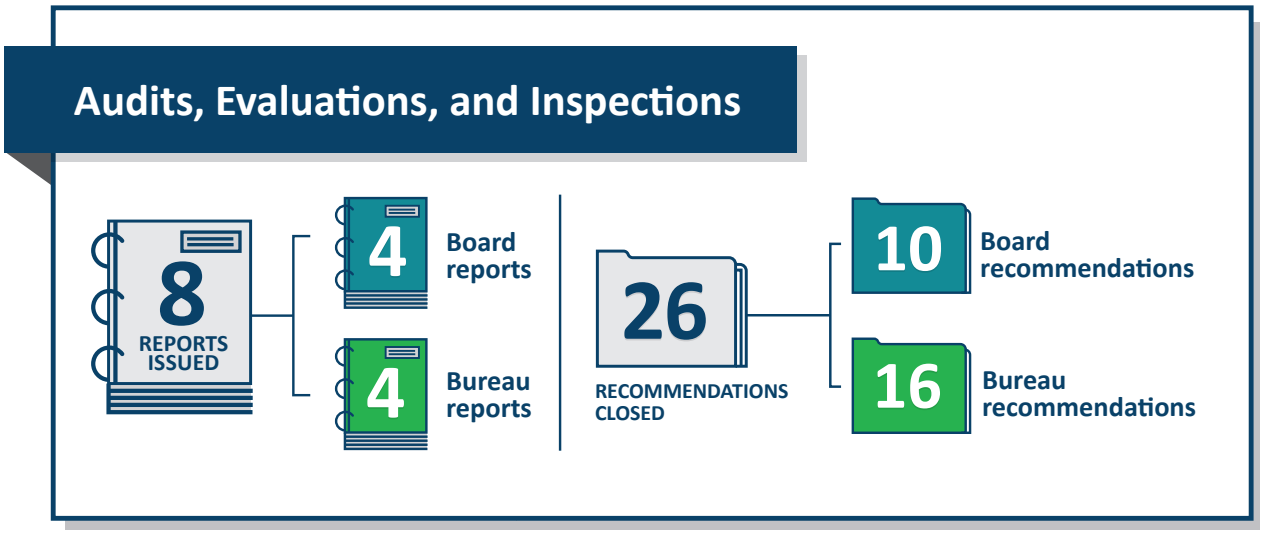
Sincerely,

Mark Bialek
Inspector General
October 31, 2018

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 Reserve Banks' Reliance on the Primary Federal Regulator of the Insured Depository Institution in the Consolidated Supervision of Regional Banking Organizations

Federal Reserve Banks appear to have increased their reliance on the primary federal regulators (PFRs) in the supervision of regional banking organizations (RBOs), but document sharing among the Board, the Reserve Banks, and the PFRs can be improved.

The Bureau's Management of Its GMMB Contract

The Bureau competitively awarded the GMMB blanket purchase agreement (BPA) and performed technical and price reasonableness evaluations in compliance with the *Federal Acquisition Regulation* (FAR); however, the Bureau can strengthen controls over its contracting processes to help ensure compliance with the FAR and internal policies and procedures.

The Bureau's Mosaic System

The security controls we tested for the Mosaic system were operating effectively; however, the Bureau can strengthen controls in the area of identity and access management to ensure that the security control environment for Mosaic remains effective.

The Board's Comprehensive Liquidity Analysis and Review

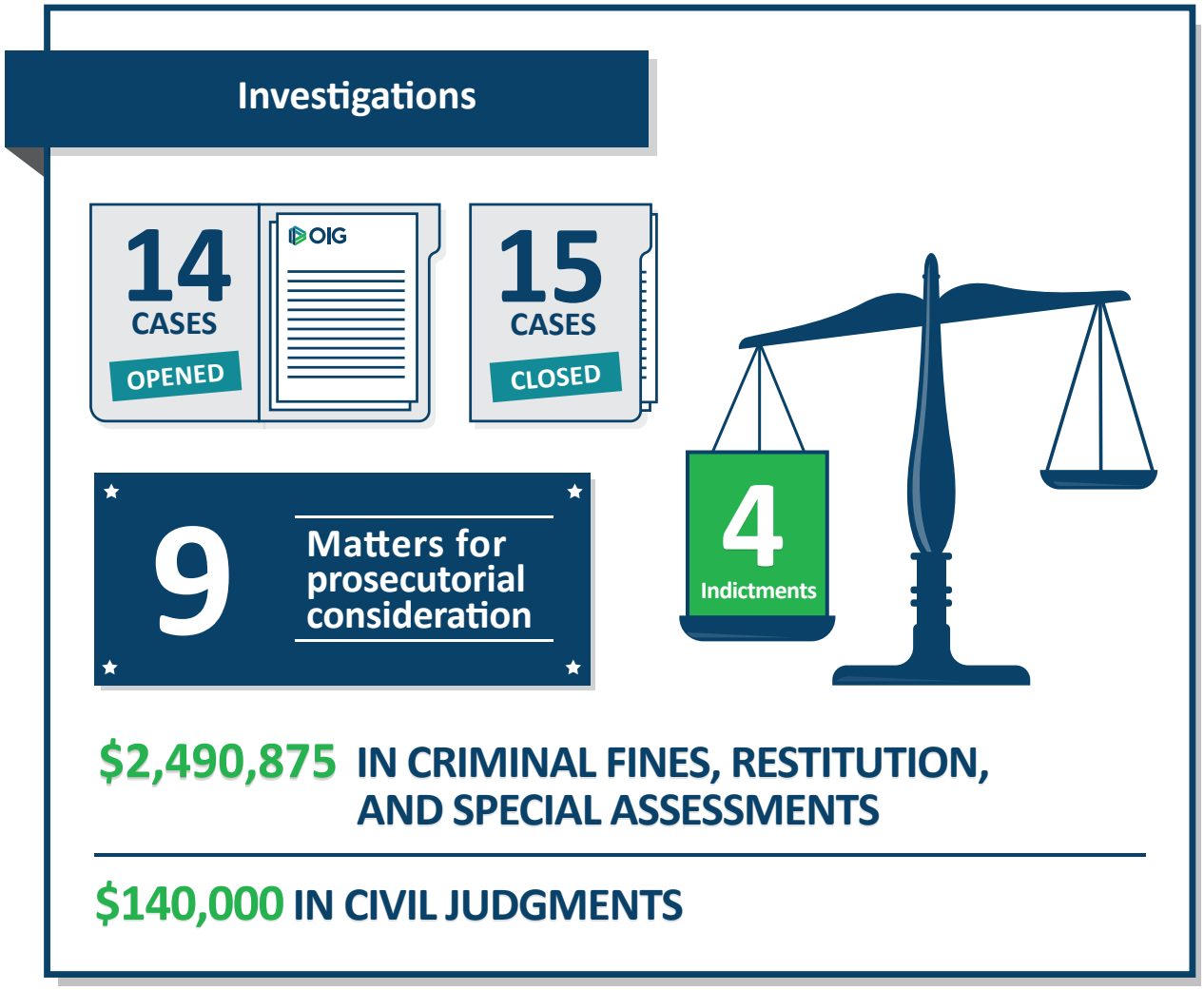
The Comprehensive Liquidity Analysis and Review (CLAR) program appears to preserve and maintain institutional knowledge related to supervisory findings and fosters effective collaboration; however, the program's knowledge management practices can be further strengthened.

The Bureau's Government Travel Card Program

Although the Bureau's government travel card (GTC) program controls are generally effective, they can be further strengthened to prevent improper reimbursements and to ensure compliance with *Federal Travel Regulation* requirements.

The Board Division of Research and Statistics' General Support System

The Division of Research and Statistics (R&S) has taken steps to implement information security controls for its general support system (GSS) in accordance with the Federal Information Security Modernization Act of 2014 (FISMA) and Board information security policies, procedures, standards, and guidelines. However, we identified opportunities for improvement in the implementation of the Board's information system security life cycle for the R&S GSS to ensure that information security controls are effectively implemented, assessed, authorized, and monitored.



Four Former Senior Executives of Wilmington Trust Convicted by Jury in Federal District Court

Former top executives of Delaware's Wilmington Trust, including its President and its Executive Vice President, were found guilty of conspiracy to defraud the United States, securities fraud, making false statements to federal agencies, and falsifying banking records. The defendants conspired to conceal the truth about Wilmington Trust's failing financial health by omitting information about past-due loans in reports to federal regulators and the investing public.

Former Bureau Examiner Sentenced for Bribery of a Public Official

A former Bureau employee was sentenced in Arizona to probation and fines for accepting a bribe in the form of a preferential home mortgage loan from a credit union. At the time, the defendant worked for

the National Credit Union Administration (NCUA) as the primary examiner of the credit union. Later hired by the Bureau, the defendant failed to disclose this financial misconduct in his application. The defendant resigned from the Bureau on the same day he entered his guilty plea.

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 NCUA, the U.S. Securities and Exchange Commission, 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 NCUA, 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.

Major Management Challenges

Although not required by statute, we annually report on the major management challenges facing the Board and the Bureau. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the Bureau's accomplishment of their strategic objectives. The agencies' 2018 challenges are similar to those for 2017.

For 2018, we identified six major management challenges for the Board:

- Enhancing Organizational Governance
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Ensuring an Effective Information Security Program
- Advancing Efforts to Improve Human Capital Management
- Remaining Adaptable to Internal and External Developments While Refining the Regulatory and Supervisory Framework
- Ensuring That Physical Infrastructure Effectively Meets Mission Needs

For 2018, we identified three major management challenges for the Bureau:

- Ensuring That an Effective Information Security Program Is in Place
- Managing the Human Capital Program
- Strengthening Controls and Managing Risks

See our website for our full management challenges reports to the Board and the Bureau.

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

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

2018-SR-B-010 **June 20, 2018**

The Board is the consolidated supervisor of bank holding companies (BHCs)—entities that own or control one or more banks. The Board delegates authority to each Reserve Bank to supervise the BHCs in the Reserve Bank's District. By law, the Reserve Banks must rely to the fullest extent possible on the work of the PFR of the BHCs' subsidiary depository institutions. We conducted this evaluation to assess the effectiveness of the consolidated supervision of RBOs. We reviewed how Reserve Banks rely on other federal regulators to conduct consolidated supervision of RBOs—each with $10–$50 billion in assets.

In accordance with applicable guidance related to consolidated supervision, the Reserve Banks relied on the respective PFR of RBOs' insured depository institutions to supervise the RBOs we sampled. We also noted that the Reserve Banks appear to have increased their reliance on the PFRs.

We identified an opportunity for the Board to establish general guidelines for reliance on PFR documents and to ensure that all examiners have access to those documents. In addition, we found that the Board and the Reserve Banks could improve document-sharing processes. Finally, several RBO executives noted the potentially avoidable regulatory burden created because RBO employees sometimes upload the same documentation to multiple systems in response to Reserve Bank and PFR documentation requests.

Our report contains recommendations designed to improve document sharing among the Board, the Reserve Banks, and the PFRs. The Board concurred with our recommendations.

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**

Through the CLAR program, the Federal Reserve System conducts a horizontal supervisory assessment of liquidity risk and risk management practices across Large Institution Supervision Coordinating Committee (LISCC) firms—the largest, most complex financial firms under Board supervision. We assessed the System's knowledge management processes, practices, and systems in support of the CLAR program.

The CLAR program's knowledge management practices generally align with many of the leading practices described in the academic studies and *Harvard Business Review* articles we reviewed related to preserving and transferring institutional knowledge. For example, CLAR leadership has fostered a culture that prioritizes knowledge management; CLAR teams practice regular, team-based collaboration; and the CLAR program uses an information-sharing application to capture, store, and share institutional knowledge. As a result, the CLAR program appears to preserve and maintain institutional knowledge related to supervisory findings and fosters effective collaboration.

Although the CLAR program has generally effective knowledge management practices, the 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.

Our report contains recommendations designed to further enhance the CLAR program's knowledge management practices. The Board concurred with our recommendations.

Security Control Review of the Board Division of Research and Statistics' General Support System

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

R&S is responsible for developing and presenting economic and financial data and analysis for the Board, the Federal Open Market Committee, and other Federal Reserve System officials. This information serves as background for the formulation and conduct of monetary, regulatory, and supervisory policy. The R&S GSS supports the research computing activities of R&S and other divisions. The components of the R&S GSS are listed on the Board's FISMA inventory as moderate-risk infrastructure systems. We evaluated the effectiveness of select security controls and techniques for the R&S GSS, as well as the system's compliance with FISMA and Board information security policies, procedures, standards, and guidelines.

Overall, we found that R&S has taken steps to implement information security controls for the R&S GSS in accordance with FISMA and Board information security policies, procedures, standards, and guidelines. For example, we found that the division has implemented periodic vulnerability scanning, biannual contingency testing, and a security information and event management tool to provide real-time analysis of security alerts. However, we identified opportunities for improvement in the implementation of the Board's information system security life cycle for the R&S GSS to ensure that information security controls are effectively implemented, assessed, authorized, and monitored.

Our report includes recommendations that focus on strengthening the implementation of controls and risk management activities related to access control, configuration management, and audit and accountability. The Board concurred with our recommendations.

Review of the Failure of Fayette County Bank

2018-SR-B-016 **September 26, 2018**

In accordance with the requirements of section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, we conducted an in-depth review of the failure of Fayette County Bank (FCB) because the failure presented unusual circumstances that warranted an in-depth review.

FCB failed primarily because of an aggressive growth strategy coupled with ineffective oversight by its board of directors, leading to declining asset quality and rapid capital depletion. In addition, the bank's board of directors was unable to hire and retain effective management following a long-tenured Chief Executive Officer's retirement in December 2012.

The Federal Reserve Bank of St. Louis generally took decisive supervisory action to address FCB's weaknesses and deficiencies during the time frame we reviewed, 2011 through 2017, by appropriately downgrading the bank's CAMELS composite rating consistent with its risk profile and promptly issuing an

emergency supervisory directive.[3] The Federal Reserve Bank of St. Louis's supervisory activity included formal enforcement actions and a recommendation to implement an enforcement action against an FCB bank official.

Our review resulted in a finding related to enhanced communication between the Board's Legal Division and the Federal Reserve Bank of St. Louis. Because our office has recently issued a recommendation to address that communication issue, our report contains no new recommendations.[4]

Bureau of Consumer Financial Protection

Independent Accountants' Report on the Bureau Civil Penalty Fund's 2017 Compliance With the Improper Payments Information Act of 2002, as Amended

2018-FMIC-C-009 **May 14, 2018**

IPIA requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. We contracted with an independent public accounting firm to audit the Bureau Civil Penalty Fund's compliance with IPIA for fiscal year 2017. The contract required the audit to be performed in accordance with the auditing standards applicable to performance audits contained in *Government Auditing Standards*, which is issued by the Comptroller General of the United States. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with the contract and *Government Auditing Standards*.

The independent public accounting firm determined that the Bureau complied with the two applicable requirements of IPIA for fiscal year 2017 as they relate to the Civil Penalty Fund. Specifically, the firm found that the Bureau published an annual financial statement for the most recent fiscal year, posted that report on the agency website, and conducted a program-specific risk assessment in conformance with section 2(a) of IPIA. The other four IPIA requirements are not applicable to the Civil Penalty Fund because the Bureau has determined that the fund is not susceptible to significant improper payments. The firm made no recommendations in its report.

3. The CAMELS acronym represents six components: capital adequacy, asset quality, management capability, earnings performance, liquidity position, and sensitivity to market risk. For full-scope examinations, examiners assign a rating of 1 through 5 for each component and an overall composite score, with 1 indicating the least regulatory concern and 5 indicating the greatest concern.

4. Office of Inspector General, *Review of the Failure of Allied Bank*, OIG Report 2018-SR-B-007, March 19, 2018.

The Bureau Could Have Better Managed Its GMMB Contract and Should Strengthen Controls for Contract Financing and Contract Management

2018-FMIC-C-011 **June 20, 2018**

In August 2013, the Bureau awarded a BPA to GMMB from the U.S. General Services Administration's Federal Supply Schedule for advertising and marketing services. The Bureau originally estimated that it would spend $11.5 million over 5 years. From August 2013 to February 2018, however, the Bureau obligated $43.8 million through 22 task orders under the BPA. We sampled and assessed 6 of these task orders and the related invoices—which totaled $36 million in obligations and $31.1 million in payments—to assess the Bureau's compliance with applicable laws, regulations, and internal policies and procedures related to the award and management of its contract with GMMB for advertising and marketing services.

The Bureau competitively awarded the GMMB BPA and performed technical and price reasonableness evaluations in compliance with the FAR. However, the Bureau can improve controls to help ensure compliance with the FAR and internal policies and procedures. Specifically, the Office of the Chief Procurement Officer did not comply with the FAR requirements for contract financing and annual BPA reviews. Complying with contract financing requirements and fully conducting and documenting annual BPA reviews could help ensure and provide evidence that contracts awarded or option periods exercised are in the best interest of the government and that the Bureau administers its contracts in compliance with the FAR.

In addition, the program office involved with the BPA did not timely communicate with the Office of the Chief Procurement Officer about the use of contract financing, did not properly monitor the liquidation of prepaid media purchases, and did not verify actual expenses using source documents. Properly managing contracts is essential for overseeing the financial and general performance of the contract and can help reduce both the likelihood of improper payments and the Bureau's vulnerability to fraud, waste, and abuse.

Our report contains recommendations designed to strengthen the Bureau's controls over its contracting processes. The Bureau concurred with our recommendations.

Security Control Review of the Bureau's Mosaic System

2018-IT-C-012R **June 27, 2018**

Mosaic, a public-facing web application running on a cloud-based platform-as-a-service, is used by the Bureau to manage consumer complaints related to financial products and services. It also provides the Bureau with enhanced services and tools related to workforce and resource management; entity boarding; and the creation and management of investigative records, company ratings, and surveys. In

accordance with FISMA requirements, we evaluated the effectiveness of specific (1) security controls for the Mosaic system and (2) components of the planning, development, and delivery processes used for the system as they relate to the Bureau's risk management program.

Overall, we found that the security controls we tested for the Mosaic system were operating effectively. Further, specific components of the planning, development, and delivery processes used for the system, as they relate to the Bureau's risk management program, were performed effectively. For instance, we found that controls related to continuous monitoring, vulnerability scanning and remediation, and system and information integrity were operating effectively. Further, the Bureau developed a business case, which included an analysis of the benefits and risks, prior to implementing Mosaic. However, we found that the Bureau can strengthen controls in the area of identity and access management to ensure that the security control environment for Mosaic remains effective.

We made a recommendation in the area of identity and access management controls for Mosaic. The Bureau concurred with our recommendation. In addition, our report includes matters for management's consideration in the areas of audit and accountability, contingency planning, and configuration management.

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

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

Through its GTC program, the Bureau provides its employees with an individually billed GTC account to arrange and pay for official travel and related expenses. Approving officials review and approve authorized expenses, for which the Bureau then reimburses cardholders. 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. After we presented our draft findings to Bureau officials during our

audit, the agency updated its existing cost-comparison worksheet to include estimated travel time per method of transportation and communicated the update to all managers and staff.

Our report contains recommendations designed to help ensure GTC program integrity. 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. During the reporting period, we completed our review of the failure of FCB. A summary of our findings can be found in the Audits, Evaluations, and Inspections section of this report.

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 BHCs, 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 BHCs and state member banks, and the Board's Division of Supervision and Regulation oversees the Reserve Banks' supervisory activities.

Our office's investigations concerning BHCs 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 Chief Executive Officer and President Sentenced for Conspiracy to Commit Bank Fraud and Obstruction of Examination

A former Chief Executive Officer and President at Coastal Bank and Trust, a state member bank based in Jacksonville, North Carolina, was sentenced in the U.S. District Court in the Eastern District of North

Carolina to 48 months in prison for one count of conspiracy to commit bank fraud and one count of obstruction of examination. The court ordered the term of imprisonment to be followed by 3 years of supervised release. The defendant was also ordered to pay $2,397,475 in restitution.

The defendant engaged in a scheme to defraud Coastal Bank and Trust by engineering fraudulent loan transactions to straw borrowers while the true beneficiaries of these loans were coconspirators of the defendant, business entities controlled by the defendant, or the defendant himself. The defendant used his position of trust and authority at the bank to circumvent the bank's internal controls and normal loan underwriting procedures. The defendant concealed his scheme to defraud by withholding relevant information about the fraudulent loans that he was approving from the bank's board of directors and from Reserve Bank examiners.

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

Four Former Senior Executives of Wilmington Trust Convicted by Jury in Federal District Court

A jury in the U.S. District Court for the District of Delaware returned a guilty verdict against four former executives of Wilmington Trust Bank in Wilmington, Delaware, including the President and Chief Operating Officer, the Executive Vice President and Chief Financial Officer, the Chief Credit Officer, and the Controller.

The jury 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 U.S. Securities and Exchange Commission (SEC), making false entries in banking records, and making false statements to the SEC and the Federal Reserve. 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 Federal Reserve 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, and the Office of the Special Inspector General for the Troubled Asset Relief Program.

Former Acting President of CFG Community Bank Pleaded Guilty to Bank Fraud and Income Tax Evasion

A former acting President of CFG Community Bank, a state member bank, pleaded guilty in the U.S. District Court for the District of Maryland to one count of bank fraud and one count of income tax evasion. The defendant agreed that the court will order restitution to CFG for $892,541.75. The defendant also stipulated that restitution to the Internal Revenue Service is $365,228.80.

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.

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

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. The following is an example from this reporting period of an investigation into matters affecting the Bureau's ability to carry out its supervisory responsibilities.

Former Bureau Examiner Sentenced for Bribery of a Public Official

A former Bureau Examiner was sentenced in the U.S. District Court for the District of Arizona to 24 months' probation for one count of bribery of a public official. The defendant pleaded guilty to the violation as part of a plea agreement. The defendant was also ordered to pay a special assessment of $100 and a criminal fine of $4,300.

While the defendant worked for the NCUA as a Credit Union Examiner, he accepted a preferential home mortgage loan from a credit union. At the time the defendant received the loan, he was assigned as the primary examiner of that credit union. Based on his financial history, the defendant would not have been able to qualify for the loan from other sources. The defendant was later hired by the Bureau as an Examiner. The defendant failed to disclose the financial misconduct in his application. The defendant resigned from the Bureau on the same day he entered his guilty plea.

This case was investigated by our office and the NCUA OIG and prosecuted by the U.S. Attorney's Office for the District of Arizona.

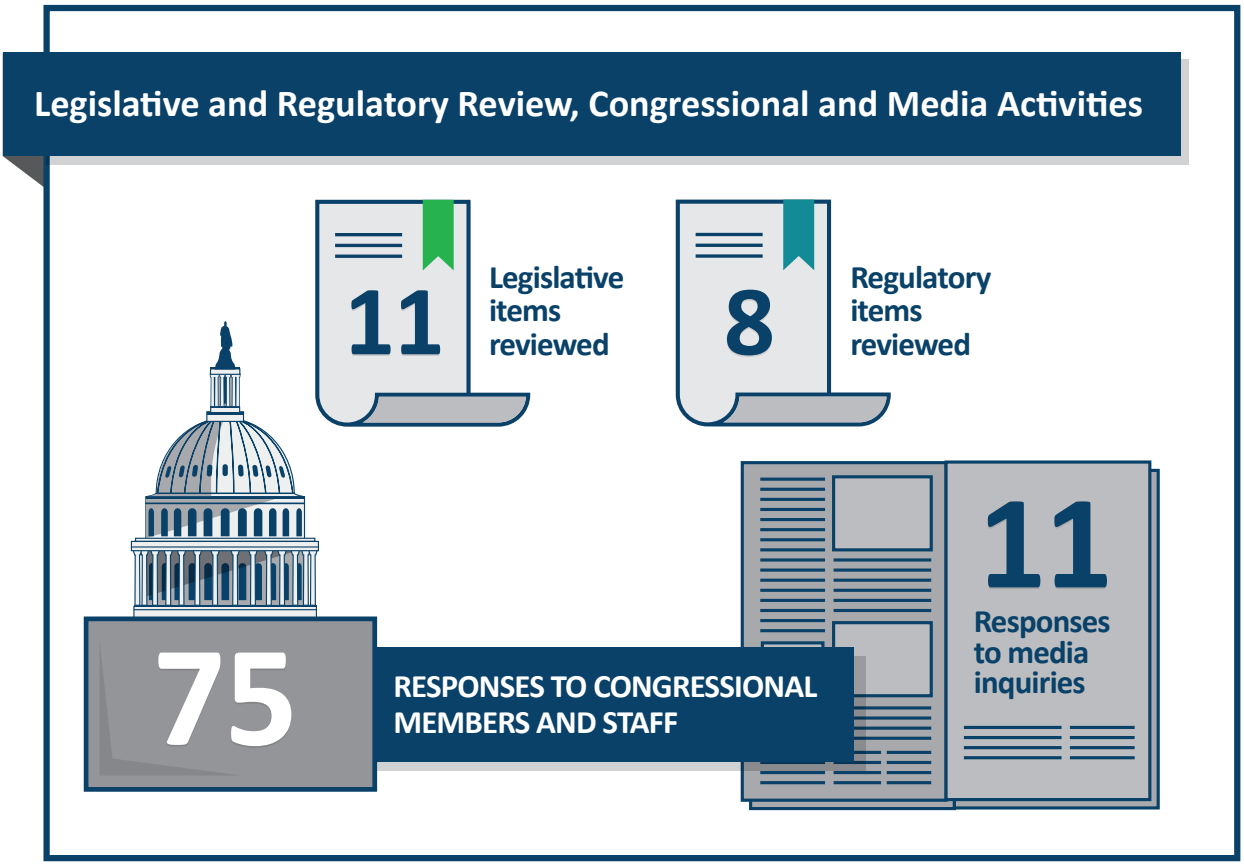
Hotline

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 272 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 8 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 75 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 11 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 9,869 reports, detailing for fiscal year 2018 alone over $27 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 and Investigations 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.

Our Associate Inspector General for Information Technology, as the Chair of the Information Technology Committee of the Federal Audit Executive Council, works with information technology audit staff throughout the OIG community and reports to the CIGIE Information Technology Committee on common information technology 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 2018, we completed a peer review of the audit organization of the Nuclear Regulatory Commission OIG. The Nuclear Regulatory Commission OIG received a rating of *pass*, and there were no report recommendations.
- 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
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	Evaluation
Knowledge Management for the Board's Comprehensive Liquidity Analysis and Review Is Generally Effective and Can Be Further Enhanced	Evaluation
Security Control Review of the Board Division of Research and Statistics' General Support System	Audit
Review of the Failure of Fayette County Bank	Evaluation
Total number of audit reports: 1	
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	03/18	0	2
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	0	09/16	7	1
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	0	03/18	0	1
Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	07/14	3[a]	3	0	06/18	2	1

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
Opportunities Exist to Enhance the Board's Oversight of Future Complex Enforcement Actions	09/14	5	5	0	09/18	5	0
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle	12/14	3	3	0	03/17	2	1
Review of the Failure of Waccamaw Bank	03/15	5	5	0	09/18	3	2
Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)	09/15	3	3	0	n.a.	0	3
Security Control Review of the Board's Statistics and Reserves System (nonpublic report)	12/15	6	6	0	11/17	6	0
The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations	04/16	9	9	0	09/18	8	1

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
Security Control Review of the Board's Active Directory Implementation (nonpublic report)	05/16	10	10	0	02/18	1	9
2016 Audit of the Board's Information Security Program	11/16	9	9	0	10/17	5	4
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	0	09/18	2	9
The Board Can Improve Documentation of Office of Foreign Assets Control Examinations	03/17	2	2	0	07/18	0	2
The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool	03/17	2	2	0	09/18	1	1
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	08/18	0	8

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 Can Strengthen Its Guidance and Planning Efforts for Future Evaluations of the Law Enforcement Unit	08/17	3	3	0	08/18	3	0
2017 Audit of the Board's Information Security Program	10/17	9	9	0	n.a.	0	9
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	n.a.	0	14
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	n.a.	0	2
Security Control Review of the Board's Public Website (nonpublic report)	03/18	7	7	0	n.a.	0	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
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	n.a.	0	3
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

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
Independent Accountants' Report on the Bureau Civil Penalty Fund's 2017 Compliance With the Improper Payments Information Act of 2002, as Amended	Audit
The Bureau Could Have Better Managed Its GMMB Contract and Should Strengthen Controls for Contract Financing and Contract Management	Audit
Security Control Review of the Bureau's Mosaic System	Audit
The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened	Audit
Total number of audit reports: 4 Total number of evaluation reports: 0	

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	08/18	13	1
Security Control Review of the CFPB's Cloud Computing–Based General Support System (nonpublic report)	07/14	4	4	0	04/18	3	1
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	10/17	2	1
The CFPB Can Enhance Its Diversity and Inclusion Efforts	03/15	17	17	0	03/18	16	1
The CFPB Can Enhance Its Contract Management Processes and Related Controls	09/15	10	10	0	05/18	10	0
Collecting Additional Information Can Help the CFPB Manage Its Future Space-Planning Activities	02/16	1	1	0	09/18	1	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 Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	0	08/18	6	3
2016 Audit of the CFPB's Information Security Program	11/16	3	3	0	10/17	1	2
The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information	05/17	9	9	0	06/18	8	1
Security Control Review of the CFPB's Public Website (nonpublic report)	05/17	8	8	0	01/18	2	6
The CFPB Can Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-Job Training Program	09/17	9	9	0	03/18	3	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
The CFPB Generally Complies With Requirements for Issuing Civil Investigative Demands but Can Improve Certain Guidance and Centralize Recordkeeping	09/17	3	3	0	09/18	3	0
The CFPB Can Improve Its Examination Workpaper Documentation Practices	09/17	17	17	0	09/18	0	17[a]
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	06/18	1	6
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	09/18	2	9
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	n.a.	0	2

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 Bureau Could Have Better Managed Its GMMB Contract and Should Strengthen Controls for Contract Financing and Contract Management	06/18	7	7	0	09/18	1	6
Security Control Review of the Bureau's Mosaic System (nonpublic report)	06/18	1	1	0	n.a.	0	1
The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened	09/18	4	4	0	n.a.	0	4

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. One of these recommendations was closed on October 1, 2018.

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	57
Investigations opened during the reporting period	14
Investigations closed during the reporting period	15
Investigations open at end of the reporting period	56
Investigative results for the reporting period	
Persons referred to U.S. Department of Justice prosecutors	9
Persons referred to state/local prosecutors	0
Declinations received	4
Joint investigations	32
Reports of investigation issued	3
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	1
Suspensions	0
Debarments	0
Prohibitions from banking industry	2
Indictments	4
Criminal informations	0
Criminal complaints	1

See notes at end of table.

Investigative actions	Number or dollar value[a]
Convictions	7
Civil actions	$0
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$140,000
Criminal fines, restitution, and special assessments	$2,490,875
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	22
Complaints received during reporting period	272
Total complaints for reporting period	294
Complaints resolved during reporting period	267
Complaints pending	27

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 have no such instances to report.

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	4	23
2017	5	34
2018[a]	6	26

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 September 30, 2018.

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[5]
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

5. 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.

The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations

2016-MO-B-006 **April 15, 2016**

Total number of recommendations: 9
Recommendations open: 1

We assessed the Board's controls to protect sensitive economic information from unauthorized disclosure when it is provided under embargo to news organizations either through a press lockup room located at the Board or through the Board's embargo application.

We identified opportunities for the Board (1) to more strictly adhere to controls already established in policies, procedures, and agreements with participating news organizations and (2) to establish new controls to more effectively safeguard embargoed economic information. We also identified risks to providing information under embargo through the embargo application.

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: 4

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: 9

We initiated this evaluation in response to a written request from the Director of the Board's Division of Banking Supervision and Regulation[6] 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 LISCC firms and large banking organizations (LBOs) 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 LISCC firms and LBOs.

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 Improve Documentation of Office of Foreign Assets Control Examinations

2017-SR-B-003 **March 15, 2017**

Total number of recommendations: 2
Recommendations open: 2

We evaluated the Board's supervision activities for foreign banking organizations following high-profile enforcement actions related to Office of Foreign Assets Control (OFAC) violations. Our objective was to assess the Board's approach to evaluating foreign banking organizations' OFAC compliance programs.

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

The OFAC examinations we reviewed did not always include documentation to adequately explain the rationale for the examination approach or the basis for conclusions. Although the *Examination Manual for U.S. Branches and Agencies of Foreign Banking Organizations* includes guidance on what to include in examination workpapers and the *Bank Secrecy Act/Anti-Money Laundering Examination Manual* includes OFAC examination procedures, there was no guidance or minimum expectations specific to how OFAC examinations should be documented. We also found data reliability concerns in the National Examination Database regarding whether OFAC compliance had been reviewed. These data reliability concerns may have occurred because there was no established definition of what it means to review OFAC compliance and because Reserve Banks did not have consistent data entry procedures. In addition, the National Examination Database did not capture data that would have indicated the extent of coverage of OFAC examinations.

The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool

2017-SR-B-005 **March 29, 2017**

Total number of recommendations: 2
Recommendations open: 1

We assessed the effectiveness of continuous monitoring as a supervisory activity for large, complex financial institutions, including LISCC firms and LBOs.

Although the Board and the Reserve Banks had multiple documents that address the expectations for certain aspects of continuous monitoring, the Board had not issued guidance that harmonizes these expectations across its supervisory portfolios and the Reserve Banks. Such guidance could have outlined the preferred analytical approach and documentation practices for this activity across the LISCC and LBO supervisory portfolios and minimized the variability that we noted for continuous monitoring activities across the Reserve Banks we visited. Although we noted certain best practices for executing continuous monitoring during our evaluation, those practices had not been broadly implemented across the Federal Reserve System. As a result, supervisory guidance issued by the Board could have helped to foster more-consistent execution of this supervisory activity throughout the Federal Reserve System and to maximize its effectiveness.

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: 8

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, (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: 9

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 information technology 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: 14

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.

Review of the Failure of Allied Bank

2018-SR-B-007 **March 19, 2018**

Total number of recommendations: 2
Recommendations open: 2

After more than 100 years in business, Arkansas-based Allied Bank failed in 2016, resulting in an estimated $6.9 million loss to the DIF. In accordance with the Dodd-Frank Act, we conducted an in-depth review of the bank's failure.

Allied Bank failed because of corporate governance weaknesses and asset quality deterioration resulting from deficient credit risk-management practices. Although the Federal Reserve Bank of St. Louis took decisive supervisory action to address Allied Bank's weaknesses, it could have also recommended that the Board report suspicious activity to law enforcement when the Reserve Bank first identified signs of insider abuse. Our review resulted in a finding related to Suspicious Activity Report filings by the Federal Reserve System and a finding related to enhanced communication between the Board's Legal Division and the Reserve Banks.

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.

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

2018-SR-B-010 **June 20, 2018**

Total number of recommendations: 3
Recommendations open: 3

See the summary in the body of this report.

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

See the summary in the body of this report.

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

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	2	2
2015	1	1
2016	2	5
2017	5	36
2018[a]	5	22

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 September 30, 2018.

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 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.

Security Control Review of the CFPB's Cloud Computing–Based General Support System (nonpublic report)

2014-IT-C-010 **July 17, 2014**

Total number of recommendations: 4
Recommendations open: 1

We reviewed the information system security controls for the Bureau's cloud computing–based GSS.

Overall, we found that the Bureau had taken a number of steps to secure its cloud computing–based GSS in accordance with FISMA requirements. However, we found that improvements were needed to ensure effective and consistently implemented FISMA processes and controls across all information security areas for the GSS.

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: 2

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 information technology infrastructure from Treasury.

The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information

2017-SR-C-011 **May 15, 2017**

Total number of recommendations: 9
Recommendations open: 1

We evaluated the Bureau Office of Enforcement's processes for protecting sensitive information to determine whether it has effective controls to manage and safeguard access to its confidential investigative information.

We found that the Office of Enforcement's sensitive information had not always been restricted to Office of Enforcement employees who needed access to that information to perform their assigned duties. This situation was due to the Office of Enforcement's challenges with updating access rights, as well as complications resulting from an information technology system migration. During our fieldwork, the Office of Enforcement took several steps to improve its approach to restricting access.

We also found that the Office of Enforcement did not follow some aspects of the Bureau's document labeling and storage requirements for handling and safeguarding sensitive information. Finally, we found that the Office of Enforcement used inconsistent naming conventions for matters across its four electronic applications and two internal drives, which hinders its ability to verify, maintain, and terminate access to files and to efficiently locate documents and data in matter folders. During our fieldwork, the Office of Enforcement took steps to improve its storage of sensitive information and its use of a consistent naming convention.

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

2017-IT-C-010 **May 22, 2017**

Total number of recommendations: 8
Recommendations open: 6

We audited selected security controls for protecting the Bureau's consumerfinance.gov website, as well as for compliance with FISMA and other federal and Bureau information security policies, procedures, standards, and guidelines.

Although we found that the Bureau had taken a number of positive steps to secure consumerfinance.gov, several control deficiencies needed to be mitigated to protect the website. Those deficiencies had to do with configuration management, system and information integrity, and contingency planning. We also identified additional risks related to system and communications protection, audit and accountability, identification and authentication, system and information integrity, and configuration management.

The CFPB Can Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-Job Training Program

2017-SR-C-014 **September 20, 2017**

Total number of recommendations: 9
Recommendations open: 6

We evaluated the effectiveness of the Bureau's management of the Examiner Commissioning Program (ECP) and the On-the-Job Training program.

Although the Bureau has taken steps to enhance the ECP since its implementation in October 2014, we identified additional ways in which the agency could improve the program. First, some examiners appeared to be pursuing components of the ECP before being fully prepared. Second, some examiners did not appear to receive adequate training or developmental opportunities and exposure to certain Bureau internal processes before starting certain components of the ECP. Third, the Bureau did not have a formal method to evaluate and update the ECP. Fourth, the Bureau did not consistently communicate ECP requirements to prospective employees. Fifth, the ECP policy should be updated to clarify when the 5-year time requirement for examiners' obtaining their commissioning begins. Finally, the Bureau could enhance its implementation of the On-the-Job Training program. Specifically, Bureau regions have not consistently implemented the program, and examiners have not clearly understood the requirements, expectations, and purpose of the program.

The CFPB Can Improve Its Examination Workpaper Documentation Practices

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

Total number of recommendations: 17
Recommendations open: 17[7]

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.

7. One of these recommendations was closed on October 1, 2018.

We found that, subject to certain conditions being met, the Bureau Division of Supervision, Enforcement and Fair Lending'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: 6

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: 9

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 information technology 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 Could Have Better Managed Its GMMB Contract and Should Strengthen Controls for Contract Financing and Contract Management

2018-FMIC-C-011 **June 20, 2018**

Total number of recommendations: 7
Recommendations open: 6

See the summary in the body of this report.

Security Control Review of the Bureau's Mosaic System (nonpublic report)

2018-IT-C-012R **June 27, 2018**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

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

See the summary in the body of this report.

Abbreviations

BHC	bank holding company
Board	Board of Governors of the Federal Reserve System
BPA	blanket purchase agreement
Bureau	Bureau of Consumer Financial Protection
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
ECP	Examiner Commissioning Program
FAR	*Federal Acquisition Regulation*
FBI	Federal Bureau of Investigation
FCB	Fayette County Bank
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
GSS	general support system
GTC	government travel card
IG	Inspector General
IPIA	Improper Payments Information Act of 2002, as amended
LBO	large banking organization
LISCC	Large Institution Supervision Coordinating Committee
MDPS	multiregional data processing servicer
NCUA	National Credit Union Administration
NRAS	National Remote Access Services
OCC	Office of the Comptroller of the Currency

OFAC	Office of Foreign Assets Control
OIG	Office of Inspector General
PFR	primary federal regulator
RADAR	Risk Assessment, Data Analysis, and Research
R&S	Division of Research and Statistics
RBO	regional banking organization
SEC	U.S. Securities and Exchange Commission
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