Office of Inspector General

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

Semiannual Report to Congress

October 1, 2019–March 31, 2020

OIG

Semiannual Report to Congress

October 1, 2019–March 31, 2020

Office of Inspector General

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

Message From the Inspector General

Needless to say, the world has changed significantly since our previous semiannual report to Congress. The COVID-19 global pandemic has transformed not only how we work, but also how we care for our children, stay connected to family and friends, and participate in our communities. Along with the concern we feel for our health and safety are the disruptions to the rhythms of our lives—to birthday parties, weddings, vacations, commencements, and more.

The pandemic of course has also created substantial economic uncertainty. In response, Congress has passed the Coronavirus Aid, Relief, and Economic Security Act, or CARES Act, which provides more than $2 trillion in emergency federal spending to address the economic effects of the pandemic. The CARES Act also establishes the Pandemic Response Accountability Committee to coordinate oversight of federal funds used for the coronavirus response. I am serving on the committee along with 20 other inspectors general. Together, we will work to ensure that the largest aid package in American history is used effectively and is free of fraud, waste, and abuse.

In response to the heightened economic uncertainty, the Board of Governors of the Federal Reserve System has taken steps to support the flow of credit to U.S. households and businesses. The Bureau of Consumer Financial Protection is engaged in consumer education efforts related to coronavirus scams. In these challenging times, our independent oversight of the Board and the Bureau is vital. Whether working from our offices or from our homes, we are committed to our mission.

During the past 6 months, we issued reports related to the Board's programs and operations that address the information security program, the financial statements of the Board and the Federal Financial Institutions Examination Council, postemployment restrictions for senior examiners, the designated financial market utility supervision program, enforcement action monitoring practices, the operating budget process, the Protective Services Unit, and contract administration. We issued reports on the Bureau's programs and operations that address the information security program and final order follow-up activities.

We also issued three memorandum reports (available publicly in summary form only) discussing the results of the technical testing we conducted as part of our annual Federal Information Security Modernization Act of 2014 (FISMA) review of the effectiveness of the Board's and the Bureau's information security programs. These reports cover the Board's data loss protection solution, the

Bureau's cybersecurity incident response process, and the Bureau's data exfiltration controls. Although conducting technical testing as part of our annual FISMA reports is not new for us, we have begun issuing these detailed memorandums to help the Board and the Bureau address our recommendations.

We also saw results in high-profile cases related to the programs and operations of the Board and the Bureau. Wells Fargo agreed to pay $3 billion to resolve criminal and civil investigations into sales practices involving the opening of millions of accounts without customer authorization, and an employee of a mortgage company was sentenced to 46 months in prison and ordered to pay restitution for theft of $2 million from customers. We also resolved 289 hotline complaints and closed 12 investigations, and our work resulted in 9 persons referred for criminal prosecution.

I am profoundly grateful to the OIG staff, who have faced unprecedented challenges with creativity, determination, and grace. These are difficult times, and we do not yet know when this pandemic will end or what its effects will be. But for me, my team's dedication, resilience, and commitment to our mission remain a source of hope—and tremendous pride.

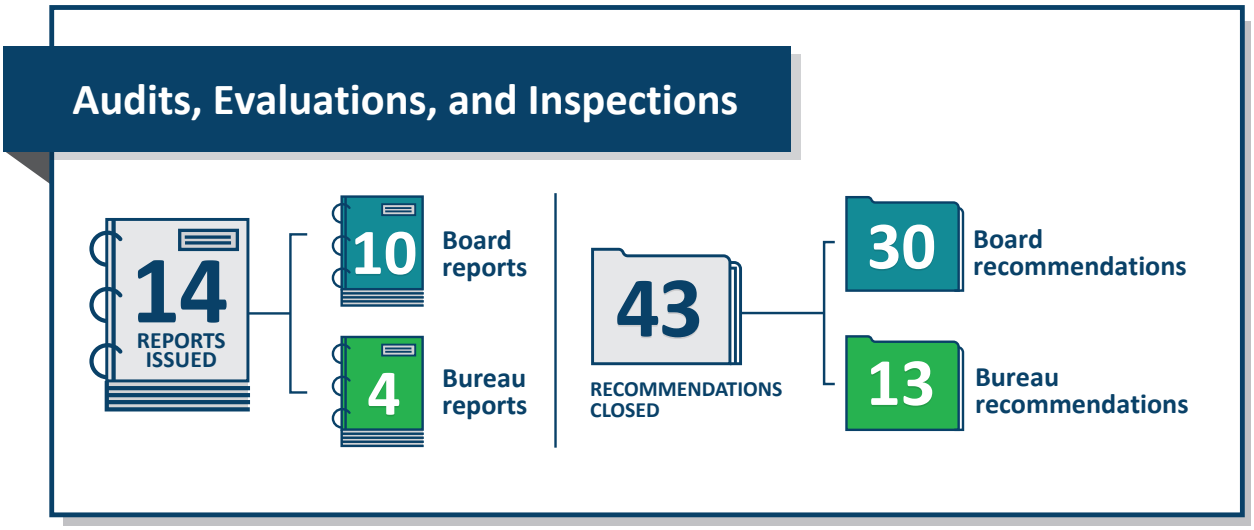
Sincerely,

Mark Bialek
Inspector General
April 30, 2020

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 and the Bureau of Consumer Financial Protection. The following are highlights, in chronological order, of our work during this semiannual reporting period.



The Board's Information Security Program

The Board's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. The Board has opportunities to mature its information security program in Federal Information Security Modernization Act of 2014 (FISMA) domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

The Bureau's Information Security Program

The Bureau's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. The Bureau has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

The Bureau's Final Order Follow-Up Activities

The Bureau has implemented some effective practices to improve its follow-up on final orders issued against an entity or person for violations of federal consumer financial law; however, we identified additional opportunities for the Bureau to improve its final order follow-up activities and reporting.

The Board's Oversight of Its Designated Financial Market Utility Supervision Program

The Board has implemented practices and processes (1) to ensure governance over the designated financial market utility (DFMU) supervision program, (2) to collaborate with other supervisory agencies in accordance with authorities provided in the Dodd-Frank Wall Street Reform and Consumer Protection Act, and (3) to conduct reviews of material changes filed by DFMUs that meet the Board's responsibilities under title VIII of the Dodd-Frank Act. However, we identified opportunities for the Board to enhance these practices and processes.

The Board's Enforcement Action Monitoring Practices

The Federal Reserve Banks in our sample have implemented some effective practices for monitoring enforcement actions designed to compel an institution to address issues identified through the supervisory process or other means; however, we identified opportunities for the Board to enhance certain aspects of these practices.

The Board's Protective Services Unit

We assessed the Internal Oversight Committee's (IOC) 2018 evaluation of Protective Services Unit (PSU) operations, as well as the PSU's compliance with its policies and procedures. The 2018 IOC evaluation generally complied with the IOC guidance, although we found opportunities for improvement that could strengthen future IOC evaluations. Similarly, our review of the PSU's operations found that it complied with its policies and procedures for certain aspects of protection measures and protective intelligence, but we found opportunities for improvement.

The Board's Contract Administration Processes

The Board awarded approximately $450 million in contracts for goods and services in 2018. Our audit identified opportunities for the Board to improve its contract administration processes as well as related internal controls.

Wells Fargo Agrees to $3 Billion Penalty for False Sales Practices

Our agents engaged in a joint investigation that resulted in Wells Fargo and Co. and its subsidiary, Wells Fargo Bank, N.A., agreeing to pay $3 billion to resolve three matters stemming from a years-long practice of pressuring employees to meet unrealistic sales goals. The practice led thousands of employees to provide millions of accounts or products to customers under false pretenses or without consent, often by creating false records or misusing customers' identities.

Mortgage Employee Sentenced for $2 Million Theft

Our agents participated in a joint investigation of a former payment processor at Freedom Mortgage who was ultimately sentenced to 46 months in federal prison and ordered to pay over $2 million in restitution after pleading guilty to money laundering and unauthorized access of a computer with intent to defraud.

Over 3 years, she diverted unclaimed escrow checks to accounts controlled by her family and friends and altered company computer records to cover her tracks.

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 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 Act (12 U.S.C. § 1831o(k)), outlines certain review and reporting obligations for our office when a state member bank failure occurs. The nature of those review and reporting requirements depends on the size of the loss to the Deposit Insurance Fund.
- 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.
- The Federal Information Security Modernization Act of 2014 (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 testing the effectiveness of security controls and practices for selected information systems.

- The Payment Integrity Information Act of 2019 (PIIA; 31 U.S.C. §§ 3351–58) 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 the PIIA. The PIIA requires us to determine each fiscal year whether the agency is in compliance with the act.
- 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 Board's and 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 Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we oversee the annual financial statement audits of the Board and of the FFIEC.[2] Under the Dodd-Frank Act, the U.S. Government Accountability Office performs the financial statement audit of the Bureau.

1. CIGFO comprises the IGs of the Board and the Bureau, the Commodity Futures Trading Commission, the U.S. Department of Housing and Urban Development, the U.S. Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, the 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 National Credit Union Administration, the Office of the Comptroller of the Currency, and the Bureau and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

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

Audits, Evaluations, and Inspections

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

Evaluations and inspections also assess aspects of the economy, efficiency, and effectiveness of Board and Bureau programs and operations. Evaluations are generally focused on the effectiveness of specific programs or functions; we also conduct our legislatively mandated reviews of failed financial institutions supervised by the Board as evaluations. Inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Our evaluations and inspections are performed according to *Quality Standards for Inspection and Evaluation*, which is 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

2019 Audit of the Board's Information Security Program

2019-IT-B-016 **October 31, 2019**

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

The Board's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. The Board has opportunities to mature its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. Similar to our previous FISMA audits, a consistent theme we noted is that the decentralization of information technology (IT) services results in an incomplete view of the risks affecting the Board's security posture. In addition, the Board has not defined

its enterprisewide risk management strategy, risk appetite, and risk tolerance levels; defining them could help guide cybersecurity processes across function areas.

The Board has taken sufficient action to close 3 of the 15 recommendations from our prior FISMA audits that remained open at the start of this audit. This report contains 6 new recommendations designed to strengthen the Board's information security program in the areas of risk management, identity and access management, and data protection and privacy. The Board concurred with our recommendations.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2019 and 2018, and Independent Auditors' Report

2020-FMIC-B-001 **February 26, 2020**

The Board performs the accounting function for the FFIEC, and we contract with an independent public accounting firm to annually audit the financial statements of the FFIEC. The contract requires the audits to be performed in accordance with auditing standards generally accepted in the United States and in accordance with the auditing standards applicable to financial audits in *Government Auditing Standards*, 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 applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the FFIEC as of December 31, 2019 and 2018, and the results of operations and cash flows for the years then ended in conformity with accounting principles generally accepted in the United States. The auditors' report on internal control over financial reporting and on compliance and other matters disclosed no instances of noncompliance or other matters.

The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction

2020-SR-B-003 **March 9, 2020**

The Intelligence Reform and Terrorism Prevention Act of 2004 restricts senior examiners at Reserve Banks from working for depository institutions and depository institution holding companies they have supervised during 2 or more months of their final 12 months of employment. The penalties for violating this restriction may include an industrywide prohibition for up to 5 years and a civil monetary penalty of up to $250,000. To implement the act, the Board issued Supervision and Regulation Letter 16-16/ Consumer Affairs Letter 16-7, *Special Post-Employment Restriction for Senior Examiners* (SR Letter 16-16).

We assessed the effectiveness of controls designed to ensure compliance with the requirements outlined in SR Letter 16-16.

We found that the four Reserve Banks in our sample have issued policies and procedures to identify senior examiners, require that they be notified of their postemployment restriction, and require workpaper reviews as appropriate. These Reserve Banks took different approaches, however, to determining whom to designate as a *senior examiner*. The senior examiners we interviewed appeared to understand the postemployment restriction and the penalties for violating the restriction.

Although the Board found through a 2017 horizontal review that the Reserve Banks implemented the Board's postemployment restriction guidance, the review also found that the Reserve Banks did not always apply the *senior examiner* definition in accordance with the guidance. Thus, the 2017 review team recommended that the Board issue additional guidance to clarify the definition of a *senior examiner*. As of November 2019, the Board had not finalized this guidance.

Our report contains a recommendation designed to enhance the consistency among Reserve Banks in determining which employees should be designated as *senior examiners* for the purpose of applying the postemployment restriction. The Board concurred with our recommendation.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2019 and 2018, and Independent Auditors' Report

2020-FMIC-B-004 **March 11, 2020**

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

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2019 and 2018, and the results of its operations and its cash flows for the years then ended in conformity with accounting principles generally accepted in the

United States. Also, in the auditors' opinion, the Board maintained, in all material respects, effective internal control over financial reporting as of December 31, 2019, based on the criteria established in *Internal Control—Integrated Framework* (2013) by the Committee of Sponsoring Organizations of the Treadway Commission. The auditors' report on compliance and other matters disclosed no instances of noncompliance or other matters.

The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved

2020-FMIC-B-005 **March 18, 2020**

Title VIII of the Dodd-Frank Act was enacted to mitigate systemic risk in the financial system and promote financial stability, in part through enhanced supervision of DFMUs, which are systems that transfer, clear, or settle payments and other transactions among financial institutions. A failure or disruption of a DFMU could affect the smooth functioning of financial markets or financial stability. Title VIII grants the Board enhanced authority to supervise the DFMUs for which it is the supervisory agency and to consult with other federal agencies when the Board is not the designated supervisory agency for a DFMU. We assessed the effectiveness of the Board's oversight of its DFMU supervision program.

The Board has implemented practices and processes (1) to ensure governance over the DFMU supervision program, (2) to collaborate with other supervisory agencies in accordance with authorities provided in the Dodd-Frank Act, and (3) to conduct reviews of material changes filed by DFMUs that meet the Board's responsibilities under title VIII of the Dodd-Frank Act. However, we identified opportunities for the Board to enhance these practices and processes. Specifically, we found that the Board should publish certain internal delegations of authority and define certain roles and responsibilities within the DFMU supervision program. We also found that the Board can enhance its processes for collaborating with other supervisory agencies. Lastly, we found that the Board can better prepare for emergency changes filed by the DFMUs for which it is the supervisory agency.

Our report contains recommendations designed to enhance the efficiency and effectiveness of the Board's governance over its DFMU supervision program, its collaboration with other supervisory agencies, and its processes for reviewing emergency changes filed by DFMUs. The Board concurred with our recommendations.

The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices

2020-SR-B-006 **March 18, 2020**

The Board delegates to each Reserve Bank the authority to supervise certain financial institutions within its District, with oversight by the Board's Division of Supervision and Regulation. If the Board or a Reserve Bank identifies significant concerns through the supervisory process or other means, supervision staff can use various enforcement tools to compel the institution's management to address the issues. Each Reserve Bank is responsible for monitoring compliance with all enforcement actions and recommending termination or modification of the actions within its District's purview. We assessed the effectiveness of the Board's and the Reserve Banks' enforcement action monitoring practices, with a focus on supervised financial institutions within the community banking organization (CBO) and the large and foreign banking organization portfolios.

We found that the Reserve Banks in our sample have implemented some effective practices for monitoring enforcement actions; however, we identified opportunities for the Board to enhance certain aspects of these practices. Specifically, we found that the Reserve Banks in our sample use different information systems for monitoring enforcement actions against institutions in the CBO portfolio. We learned that the Board currently has an initiative underway to develop a common technology platform for supervisory activities across the Federal Reserve System for institutions with less than $100 billion in total assets, including CBOs. We also identified certain instances of Reserve Bank staff not posting supervised institutions' progress reports describing their enforcement action remediation efforts to the required system of record.

Our report contains a recommendation designed to enhance the effectiveness of the Board's enforcement action monitoring practices. The Board concurred with our recommendation.

Testing Results for the Data Loss Protection Solution Used by the Board

2020-IT-B-009R **March 25, 2020**

As part of our 2019 audit of the Board's information security program, which we performed to meet FISMA requirements, we tested select components of the data loss protection (DLP) solution used by the Board.

Our testing identified opportunities to strengthen DLP processes to provide greater assurance that sensitive Board data are protected. We also found that the DLP solution does not monitor traffic across all parts of the Board's network nor operate consistently across all the agency's standard web browsers. Our 2019 FISMA report includes a recommendation to strengthen controls in these areas—specifically, that

the chief information officer work with the Federal Reserve System to ensure that the DLP replacement solution (1) functions consistently across the Board's technology platforms and (2) supports rulesets that limit the exfiltration weaknesses we identified, to the extent practicable. We did not make any new recommendations.

The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process

2020-FMIC-B-010 March 25, 2020

Although the Board is not subject to federal budget-related laws, it prepares an annual budget as part of its efforts to ensure appropriate stewardship and accountability. The Board's 2018 annual operating budget was $766.7 million and included 2,847 authorized positions. We assessed the design and implementation of the Board's processes for formulating and executing its annual operating budget.

The Board has made changes over the past several years to improve its budget process; the Board has acknowledged perennial underspending and is addressing it by focusing on slowing growth and spending more consistently with budget estimates. The Board can further enhance the design and implementation of its operating budget process by communicating its budget process in an overarching document, strengthening the connection between budget and strategy, and implementing an agencywide approach to executing the approved budget. Doing so may help the Board define a more predictable and repeatable process; prioritize funding and monitor progress against strategic goals; and allocate financial and human capital resources more effectively, including conducting tradeoffs across the agency.

Our report contains recommendations designed to help the Board enhance the design and implementation of its operating budget process. The Board concurred with our recommendations.

The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes

2020-MO-B-011 March 25, 2020

The mission of the PSU is to ensure the physical security of the chair of the Board at all times. The Board's IOC is responsible for conducting inspections and evaluations of the Board's PSU. We assessed the IOC's 2018 evaluation of the PSU, as well as the PSU's operations to support its mission.

The 2018 IOC evaluation of PSU operations generally complied with the IOC guidance, although we found opportunities for improvement that could strengthen future evaluations of the PSU's operations. Specifically, we found that the IOC reviewers did not confirm whether the credentials of separated agents

had been destroyed and documented, nor did they complete a section of a checklist that applies to certain aspects of the PSU's operations.

In our assessment of PSU operations, we found that the PSU complied with its policies and procedures for certain aspects of protection measures and protective intelligence. However, the PSU (1) does not have procedures related to vehicle maintenance, (2) does not require driving refresher training for special agents, and (3) did not consistently maintain records of destroyed credentials for separated agents. We are transmitting sensitive information related to the results of our evaluation in a separate, restricted memorandum.

Our report contains recommendations designed to strengthen the IOC's review of PSU operations and to improve the PSU's internal processes and controls associated with vehicle maintenance, driving refresher training for special agents, and the disposition of separated agents' credentials. The Board concurred with our recommendations.

The Board Can Improve Its Contract Administration Processes

2020-FMIC-B-012 **March 30, 2020**

The Board awarded approximately $450 million in contracts for goods and services in 2018. We assessed the Board's compliance with laws, regulations, and Board policies and procedures applicable to contract administration, as well as the effectiveness of the Board's internal controls related to contract administration. We focused on the Board's contract administration processes from postaward to contract closeout.

We found that the Division of Financial Management can improve its contract administration processes as well as related internal controls. Specifically, Procurement, a section within the division, has not established an effective internal control system to monitor contracting officer's representatives' (CORs) performance of their duties. CORs approved invoices that did not meet invoice approval requirements and did not submit all required contractor performance evaluation forms. Additionally, Procurement did not execute internal controls on contract modifications and COR Acknowledgment forms, nor did it extend standard purchase orders as required by policy. Further, contracting officers entered incomplete and inaccurate contract information into the relevant database, and the Division of Financial Management does not have a comprehensive contract closeout process that ensures all goods and services satisfy the contract terms.

Finally, CORs do not appear to be adequately trained to fulfill their responsibilities. COR training is not required prior to commencing COR duties, refresher training is not required by Board policy, and COR training is not tailored to various experience levels.

Our report contains recommendations designed to improve compliance with Board policies and procedures and improve the effectiveness of internal controls associated with contract administration. The Board concurred with our recommendations.

Bureau of Consumer Financial Protection

2019 Audit of the Bureau's Information Security Program

2019-IT-C-015 October 31, 2019

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

The Bureau's information security program is operating effectively at a level-4 (*managed and measurable*) maturity. We identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. Specifically, as we noted last year, the Bureau can strengthen its enterprise risk management program by defining a risk appetite statement and associated risk tolerance levels. Further, the Bureau has not identified its high-value assets and determined what governance and security program changes may be needed to effectively manage security for those assets. Additionally, we identified improvements needed in the implementation of the Bureau's security assessment and authorization processes to manage security risks prior to deploying Bureau systems. We also identified improvements needed in database security, timely remediation of vulnerabilities, and patching of mobile phone operating systems.

The Bureau has taken sufficient action to close 3 of the 10 recommendations from our prior FISMA audits that remained open at the start of this audit. This report contains 7 new recommendations designed to strengthen the Bureau's information security program in the areas of risk management, identity and access management, data protection and privacy, incident response, and contingency planning. The Bureau concurred with our recommendations.

The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed

2020-SR-C-002 **March 2, 2020**

Section 1055(a)(1) of the Dodd-Frank Act provides the Bureau or a court the authority to issue final orders against any entity or person for violations of federal consumer financial law. In August 2017, the Bureau's Office of Enforcement created a compliance team to centralize the office's follow-up activities on final orders. As of April 2019, Enforcement was responsible for monitoring compliance with final orders that collectively contained more than 3,000 provisions. We assessed the effectiveness of Enforcement's processes for monitoring and conducting follow-up activities related to final orders.

Enforcement has implemented some effective practices to improve its follow-up on final orders; however, we identified additional opportunities for Enforcement to improve its final order follow-up activities and reporting. First, we determined that Enforcement encountered challenges completing follow-up activities within the time frames established by its compliance team for 5 of 12 orders we reviewed. In addition, the enforcement actions page on the Bureau's public website provided information on the status of public enforcement actions that was prone to misinterpretation, because the website did not define the status categories or describe the purpose of the status information. After we completed our fieldwork and shared preliminary observations with the Bureau, the agency revised the status categories and indicated that it intends to provide additional clarifying information on its website. Finally, Enforcement can establish comprehensive guidance addressing expectations for conducting and documenting follow-up activities to help promote consistency.

Our report contains recommendations to improve Enforcement's follow-up activities and reporting related to final orders. The Bureau concurred with our recommendations.

Technical Testing Results of the Bureau's Data Exfiltration Controls and Related Technologies

2020-IT-C-007R **March 23, 2020**

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we completed technical testing of the Bureau's data exfiltration controls and related technologies.

Our testing found that the Bureau could improve its data exfiltration controls to better ensure the protection of sensitive agency data accessed remotely. Specifically, a technology being used by the Bureau to monitor and control data exfiltration was not consistently implemented across the agency's

IT environment. Further, this technology was not being used to block access to known public internet storage sites. These issues increase the risk of unauthorized exfiltration of sensitive Bureau data without detection. Our 2019 FISMA report includes a recommendation to strengthen controls in these areas—specifically, that the chief information officer perform a risk assessment to determine the optimal deployment of the Bureau's technology for monitoring and controlling data exfiltration to all network access points and appropriate access to internet storage sites. We did not make any new recommendations.

Testing Results of Select Bureau Cybersecurity Incident Response Processes

2020-IT-C-008R **March 23, 2020**

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested select Bureau cybersecurity incident response processes.

Our testing showed that the Bureau is not consistently categorizing information security events in its cybersecurity incident response tickets. This could negatively affect the Bureau's analysis of these events as well as the resulting responses to any confirmed security incidents. Our 2019 FISMA report includes a recommendation to strengthen controls in this area—specifically, that the chief information officer and the chief data officer ensure that data captured in security and privacy incident processes and tickets are accurate, consistent, and of high quality. We did not make any new recommendations.

Failed State Member Bank Reviews

Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act, 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. Section 38(k) also requires that we (1) semiannually report certain information on financial institutions that incur nonmaterial losses to the Deposit Insurance Fund and (2) conduct an in-depth review of any nonmaterial losses to the Deposit Insurance Fund that exhibit unusual circumstances. No state member bank failures occurred during this reporting period.

Please refer to table A-2 and appendix C for an accounting of the progress to address recommendations associated with prior failed bank reviews.

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 *Quality Standards for Investigations*, issued by CIGIE, and *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 counterparts at other financial regulatory agency OIGs to discuss matters of mutual interest, joint investigative operations, joint training opportunities, and hotline operations.

Board of Governors of the Federal Reserve System

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

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

Wells Fargo Agrees to Pay a $3 Billion Civil Monetary Penalty Resolving Criminal and Civil Investigations Into False Sales Practices

Wells Fargo and Co. and its subsidiary, Wells Fargo Bank, N.A., have agreed to pay $3 billion to resolve three matters stemming from a years-long practice of pressuring employees to meet unrealistic sales

goals, which led thousands of employees to provide millions of accounts or products to customers under false pretenses or without consent, often by creating false records or misusing customers' identities.

As part of these agreements, Wells Fargo admitted that it collected millions of dollars in fees and interest the company was not entitled to, harmed the credit ratings of certain customers, and unlawfully misused customers' sensitive personal information.

Beginning in 1998, Wells Fargo increased its focus on sales volume and reliance on annual sales growth. A core part of this sales model was the cross-sell strategy—selling existing customers additional financial products.

Wells Fargo's Community Bank, then the largest operating segment of Wells Fargo, implemented a volume-based sales model in which employees were directed and pressured to sell large volumes of products to existing customers, often with little regard to actual customer need or expected use. Onerous sales goals and management pressure led thousands of employees to engage in unethical practices and unlawful conduct—including fraud, identity theft, and the falsification of bank records—to sell products of little or no value to the customer.

Many of these practices were referred to within Wells Fargo as *gaming*. Customer signatures were forged to open accounts without authorization, PINs were created to activate unauthorized debit cards, money was moved from millions of customer accounts to unauthorized accounts, credit cards and bill pay products were opened without authorization, customers' contact information was altered to prevent them from learning of unauthorized accounts, and customers were encouraged to open accounts they neither wanted nor needed.

Despite knowledge of the illegal sales practices, Community Bank senior leadership failed to prevent and reduce these practices. To Wells Fargo management and the board of directors, they cast the problem as driven by individual misconduct instead of the sales model itself.

This investigation was conducted by our office, the U.S. Securities and Exchange Commission, the Federal Bureau of Investigation, the Federal Deposit Insurance Corporation OIG, the Federal Housing Finance Agency OIG, and the United States Postal Inspection Service. It was prosecuted by the U.S. Attorney's Offices for the Central District of California and the Western District of North Carolina and the Commercial Litigation Branch in the Civil Division of the U.S. Department of Justice.

Former SmartBank Vice President Pleaded Guilty to Embezzling Over $600,000

A former vice president of loan operations for SmartBank, a state member bank, pleaded guilty on November 26, 2019, to embezzling or misapplying more than $600,000 of the bank's funds and to filing a false tax return.

As the vice president of loan operations, the defendant's responsibilities included overseeing the entry of financial transactions in SmartBank's general ledger system. From about 2013 to 2018, she manipulated SmartBank's general ledger to fund the issuance of 60 cashier's checks totaling nearly $360,000. About $150,000 was deposited into her bank account and used to pay credit card bills, auto loan payments, and other living expenses. The rest, including about $27,000 used to purchase a travel trailer, supported her lifestyle. Further, she manipulated SmartBank's general ledger system to fraudulently reduce her home mortgage loan by more than $200,000 and her parents' home mortgage loan by $46,000. In addition, she failed to report the embezzled funds as income on her tax returns.

The defendant faces up to 30 years in prison, a $1 million fine, 5 years' supervised release, a $100 special assessment, and forfeiture and restitution.

This was a joint investigation by our office, the Federal Housing Finance Agency OIG, the Internal Revenue Service–Criminal Investigation, and the Federal Bureau of Investigation. It was prosecuted by the U.S. Attorney's Office for the Eastern District of Tennessee at Knoxville.

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.

Former Freedom Mortgage Employee Sentenced to 46 Months in Prison for Illegally Accessing Computer to Steal $2 Million

A former payment processor at Freedom Mortgage was sentenced to 46 months in federal prison after she pleaded guilty to an information charging her with one count of unauthorized access of a computer with intent to defraud and one count of money laundering. In addition to the prison term, the defendant was sentenced to 3 years of supervised release and ordered to pay $2,087,697 in restitution. Freedom Mortgage is a privately held mortgage lender of U.S. Department of Veterans Affairs, Federal Housing Administration, and conventional loans. It is supervised by the Bureau.

From April 2014 to May 2017, the defendant had access to the company's computer system as a payment processor. She discovered that some escrow checks were returned to the company as undeliverable. She admitted that she would monitor those funds by checking monthly reports to see whether the funds were ever claimed. If the money was not claimed, she recruited various relatives and friends to allow her to use their bank accounts. With that information, she used their identities to open reloadable debit/credit accounts. She accessed the company's computer system and made it appear as if the customer requested that the money be sent by wire transfer into the fraudulent accounts. After creating the request, she accessed the company's computer and approved the transfer, using a coworker's login and password.

The defendant effected approximately 580 fraudulent wire transfers—totaling more than $2 million—from her company's bank account to bank accounts and reloadable debit/credit accounts controlled by her relatives, friends, or associates. She then used the money to pay personal expenses.

This was a joint investigation by our office, the Internal Revenue Service–Criminal Investigation, the U.S. Immigration and Customs Enforcement's Homeland Security Investigations, and the U.S. Department of Housing and Urban Development OIG. It was prosecuted by the U.S. Attorney's Office for the District of New Jersey in Camden.

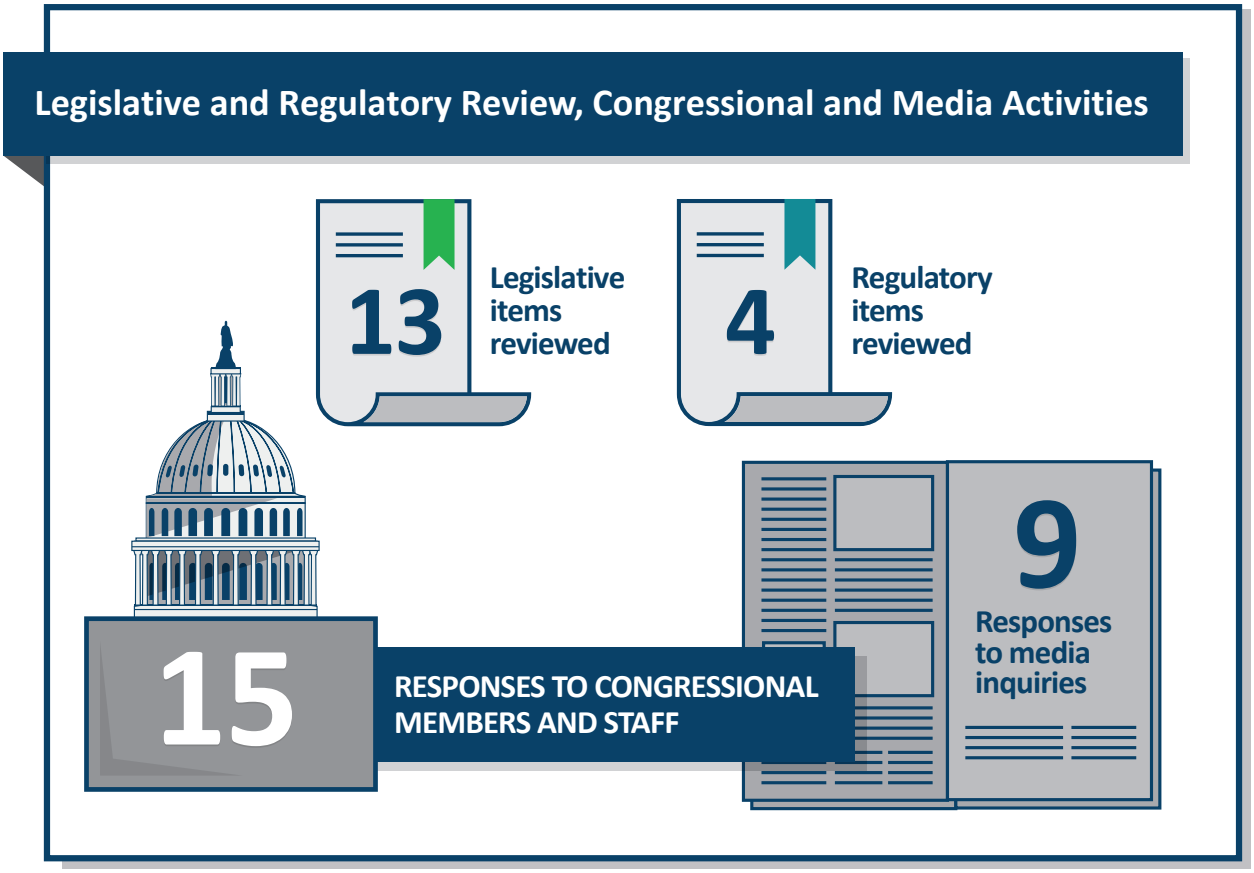
Hotline

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 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

Our Office of Legal Services 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 13 legislative items and 4 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 15 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 9 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 over 15,000 reports, detailing for fiscal year 2019 alone over $18 billion in potential savings and over 6,000 recommendations to improve programs across the federal government.

The IG serves as a member of CIGIE's Legislation Committee and Technology Committee and is the vice chair of the 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 Technology Committee facilitates effective IT audits, evaluations, and investigations and provides a forum for the expression of the OIG community's perspective on governmentwide IT operations. The Investigations Committee advises the OIG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines. In addition, the IG has been designated to serve on CIGIE's Pandemic Response Accountability Committee; the committee will coordinate oversight of federal funds authorized by the Coronavirus Aid, Relief, and Economic Security Act and the coronavirus response.

Our associate inspector general for information technology, as the chair of the Information Technology Committee of the Federal Audit Executive Council, works with IT audit staff throughout the OIG community and reports to the CIGIE Technology Committee on common IT audit issues.

Our associate inspector general for legal services and our 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. In addition, CIGIE has launched a pilot program in which inspection and evaluation units are peer reviewed by an external team every 3 years.

The Inspector General Act of 1978, as amended, requires that OIGs provide in their semiannual reports to Congress information about (1) the most recent peer reviews of their respective organizations and (2) their peer reviews of other OIGs conducted within the semiannual reporting period. The following information addresses these requirements.

- In September 2017, the National Science Foundation OIG completed the latest peer review of our audit organization. We received a peer review rating of *pass*. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our audit organization.
- In August 2019, the OIG for the Tennessee Valley Authority 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.
- In November 2019, a team comprising the OIGs for the Federal Housing Finance Agency, the Tennessee Valley Authority, and the U.S. Department of Labor completed a peer review of our evaluations policies and procedures as well as a subset of evaluations completed. No rating was assigned because the review was conducted as part of a pilot program. The review found that we sufficiently met CIGIE's *Quality Standards for Inspection and Evaluation*. There were no report recommendations, but the review team did identify suggestions to improve our compliance with internal policies and procedures.

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
2019 Audit of the Board's Information Security Program	Audit
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2019 and 2018, and Independent Auditors' Report	Audit
The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction	Evaluation
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2019 and 2018, and Independent Auditors' Report	Audit
The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved	Audit
The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices	Evaluation
Testing Results for the Data Loss Protection Solution Used by the Board	Audit
The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process	Evaluation
The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes	Evaluation
The Board Can Improve Its Contract Administration Processes	Audit
Total number of audit reports: 6 Total number of evaluation reports: 4	

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	03/20	2[a]	0
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	0	03/20	8	0
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	0	03/20	0	1
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle	12/14	3	3	0	03/20	3	0
Review of the Failure of Waccamaw Bank	03/15	5	5	0	03/20	3	2
Security Control Review of the Board's Active Directory Implementation (nonpublic report)	05/16	10	10	0	02/20	10	0
2016 Audit of the Board's Information Security Program	11/16	9	9	0	10/19	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
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	0	03/20	10	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	01/20	4	4
2017 Audit of the Board's Information Security Program	10/17	9	9	0	10/19	3	6
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	03/20	9	5
Security Control Review of the RADAR Data Warehouse (nonpublic report)	03/18	3	3	0	02/20	3	0
Security Control Review of the Board's Public Website (nonpublic report)	03/18	7	7	0	02/20	0	7
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic report)	09/18	9	9	0	03/20	7	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
2018 Audit of the Board's Information Security Program	10/18	6	6	0	10/19	1	5
Evaluation of the Board's Implementation of Splunk (nonpublic report)	11/18	1	1	0	03/20	1	0
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	n.a.	1	5
The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration	12/18	8	8	0	03/20	0	8
The Board Can Strengthen Controls Over Its Academic Assistance Program	12/18	9	9	0	01/20	4	5
The Board Can Take Additional Steps to Advance Workforce Planning	03/19	2	2	0	03/20	1	1
Leveraging Certain Strategies May Help the Board Timely Implement and Sustain Enterprisewide Workforce Planning	09/19	2	2	0	03/20	1	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
The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency	09/19	6	6	0	03/20	2	4
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	09/19	6	6	0	03/20	0	6
2019 Audit of the Board's Information Security Program	10/19	6	6	0	n.a.	0	6
The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction	03/20	1	1	0	n.a.	0	1
The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved	03/20	6	6	0	n.a.	0	6
The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices	03/20	1	1	0	n.a.	0	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
The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process	03/20	2	2	0	n.a.	0	2
The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes	03/20	6	6	0	n.a.	0	6
The Board Can Improve Its Contract Administration Processes	03/20	13	13	0	n.a.	0	13

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. Management had not provided us with sufficient evidence of its efforts to address these recommendations; thus, we have concluded that management has chosen to accept the risk of inaction. Accordingly, we closed these recommendations.

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

Report title	Type of report
2019 Audit of the Bureau's Information Security Program	Audit
The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed	Evaluation
Technical Testing Results of the Bureau's Data Exfiltration Controls and Related Technologies	Audit
Testing Results of Select Bureau Cybersecurity Incident Response Processes	Audit
Total number of audit reports: 3 Total number of evaluation reports: 1	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity	09/13	14	14	0	03/20	13	1
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	06/19	2	1
The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	0	03/20	8	1
2016 Audit of the CFPB's Information Security Program	11/16	3	3	0	07/19	2	1
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	07/19	5	2
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	03/20	9	2
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	01/20	1	1
The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened	09/18	4	4	0	03/20	0	4
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	10/19	1	3

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions	01/19	6	6	0	03/20	2	4
The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities	03/19	4	4	0	03/20	4	0
Technical Testing Results for the Bureau's SQL Server Environment (nonpublic memorandum)	05/19	5	5	0	n.a.	0	5
Bureau Efforts to Share Consumer Complaint Data Internally Are Generally Effective; Improvements Can Be Made to Enhance Training and Strengthen Access Approval	06/19	6	6	0	03/20	5	1
The Bureau Can Improve The Effectiveness of Its Life Cycle Processes for FedRAMP	07/19	3	3	0	n.a.	0	3
2019 Audit of the Bureau's Information Security Program	10/19	7	7	0	n.a	0	7
The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed	03/20	3	3	0	n.a.	0	3

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

n.a. not applicable.

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

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

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

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

Investigative actions	Number or dollar value[a]
Investigative caseload	
Investigations open at end of previous reporting period	58
Investigations opened during the reporting period	22
Investigations closed during the reporting period	12
Investigations open at end of the reporting period	68
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	10
Joint investigations	40
Reports of investigation issued	1
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	2
Suspensions	0
Debarments	0
Prohibitions from banking industry	4
Indictments	1
Criminal informations	4
Criminal complaints	0
Convictions	3
Civil actions	$0

See notes at end of table.

Investigative actions	Number or dollar value[a]
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$3,011,270,000
Criminal fines, restitution, and special assessments	$2,087,697
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	35
Complaints received during reporting period	272
Total complaints for reporting period	307
Complaints resolved during reporting period	289
Complaints pending	18

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 and the name of the senior government official, if already made public by the OIG; 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) the name of the senior government official, if already made public by the OIG; (2) a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter; (3) whether the

matter was referred to the U.S. Department of Justice and the date of the referral; and (4) 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.

- In February 2020, we closed the evaluation of the Security Assurance for the Federal Reserve program. Given recent changes to the program for securing cloud computing systems, we closed the evaluation and plan to include steps in a new evaluation related to ensuring cloud computing systems within the Reserve Banks meet the Board's information security program.
- We initiated an investigation relating to allegations that a senior government employee used government funds to purchase items for personal use. The allegations were unsubstantiated. The investigation was closed.

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
2013	1	1
2014	0	0
2015	1	2
2016	2	2
2017	3	15
2018	6	32
2019	5	18
2020[a]	6	29

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

a. Through March 31, 2020.

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

June 13, 2011

Total number of recommendations: 2
Recommendations open: 0

The minority members of the Senate Committee on Banking, Housing, and Urban Affairs requested that we review the economic analysis that the Board performed supporting five Dodd-Frank Act rulemakings. We found that 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. In addition, 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.

For several years, we have been contacting the Legal Division on a semiannual basis to follow up on these recommendations. Management had not provided us with sufficient evidence of its efforts to address these recommendations. We have concluded that management has chosen to accept the risk of inaction on these recommendations, and we closed them.

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.

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.

2016 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 1

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. 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: 1

We initiated this evaluation in response to a written request from the director of the Board's Division of Banking Supervision and Regulation[3] and the Board's general counsel. Our objectives were (1) to assess the methods for Federal Reserve System decisionmakers to obtain material information necessary to ensure that decisions and conclusions resulting from supervisory activities at Large Institution Supervision Coordinating Committee firms and large banking organizations were appropriate, supported by the record, and consistent with applicable policies and (2) to determine whether there were adequate channels for System decisionmakers to be aware of supervision employees' divergent views about material issues regarding Large Institution Supervision Coordinating Committee firms and large banking organizations.

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

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

2017-IT-B-009 **April 17, 2017**

Total number of recommendations: 8
Recommendations open: 4

We assessed (1) the Board's current cybersecurity oversight approach and governance structure, (2) the current examination practices for financial market utilities and multiregional data processing servicer (MDPS) firms for which the Board has oversight responsibilities, and (3) the Board's ongoing initiative for the future state of cybersecurity oversight. We found that the Division of Supervision and Regulation could improve the oversight of MDPS firms by (1) enforcing a reporting requirement in the Bank Service Company Act, (2) considering the implementation of an enhanced governance structure for these firms,

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

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

2017 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 6

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

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

The Board's Organizational Governance System Can Be Strengthened

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

Total number of recommendations: 14
Recommendations open: 5

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 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.

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: 2

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

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

2018 Audit of the Board's Information Security Program

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

Total number of recommendations: 6
Recommendations open: 5

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

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

The Board Can Strengthen Information Technology Governance

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

Total number of recommendations: 6
Recommendations open: 5

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

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

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

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

Total number of recommendations: 8
Recommendations open: 8

We assessed the efficiency and effectiveness of the Board's management of the currency shipment process and the effectiveness of related contracting activities.

The Board's currency shipment process is generally effective; however, the process can be enhanced to gain time and cost efficiencies. The currency forecasting process can be streamlined, and selecting different transportation modes for certain currency shipment routes and evaluating alternatives to transporting shipping equipment could yield transportation cost savings. Additionally, the Board can improve the administration of its armored carrier contracts.

The Board Can Strengthen Controls Over Its Academic Assistance Program

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

Total number of recommendations: 9
Recommendations open: 5

We assessed the adequacy of the internal controls related to the management and administration of the Board's academic assistance program.

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

The Board Can Take Additional Steps to Advance Workforce Planning

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

Total number of recommendations: 2
Recommendations open: 1

We assessed the status of enterprisewide workforce planning and related developments at the Board.

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

Leveraging Certain Strategies May Help the Board Timely Implement and Sustain Enterprisewide Workforce Planning

2019-MO-B-012 **September 25, 2019**

Total number of recommendations: 2
Recommendations open: 1

We conducted this evaluation to identify any specific operational challenges to the Board's efforts to implement workforce planning and related lessons learned from other organizations that may be applicable to the Board.

We found that although the Board has made initial progress in implementing enterprisewide workforce planning, it faces four operational challenges, which are common among other organizations in the private and public sectors: resources, data and information, time, and process ownership. Through benchmarking, we identified several strategies—having data-driven conversations, sufficient and trained resources, leadership support throughout the organization, and a clearly structured process—that may help the Board mitigate its operational challenges. We also noted that Human Resources should consider partnering with relevant divisions to coordinate workforce planning with other processes.

The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency

2019-SR-B-013 **September 25, 2019**

Total number of recommendations: 6
Recommendations open: 4

We assessed the efficiency and effectiveness of the Board's and the Reserve Banks' enforcement action issuance and termination processes and practices.

We found that the Board and the Reserve Banks have implemented some effective practices to support the enforcement action issuance and termination processes; however, we identified opportunities for the Board to enhance these processes. Specifically, we found that the Board can clarify certain

aspects of these internal processes, such as the steps in these processes, the Board stakeholders' roles and responsibilities, and the Board members' involvement. In addition, we found that the Board can (1) improve the timeliness and efficiency of its enforcement action issuance and termination processes and (2) increase transparency with respect to the status of ongoing enforcement actions.

The Board's Law Enforcement Operations Bureau Can Improve Internal Processes

2019-MO-B-014 **September 30, 2019**

Total number of recommendations: 6
Recommendations open: 6

We assessed whether the control environment in the Law Enforcement Unit's (LEU) Operations Bureau is operating effectively to support the LEU's mission as well as components of the Management Division's strategic goals.

We found that the LEU's Operations Bureau can improve standards and processes associated with its control environment to better support the LEU's mission. Specifically, we found that the LEU did not document the roles, responsibilities, training qualifications, and reporting requirements after modifying its process for internal reviews. We also found that the LEU can better communicate its decisions and the rationale for changes affecting the Operations Bureau and can take further action to improve communication generally. Additionally, the LEU can better capitalize on professional development opportunities for officers and new supervisors. Lastly, the LEU should also strengthen its processes for determining shift and post assignments.

2019 Audit of the Board's Information Security Program

2019-IT-B-016 **October 31, 2019**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction

2020-SR-B-003 **March 9, 2020**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved

2020-FMIC-B-005 **March 18, 2020**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices

2020-SR-B-006 **March 18, 2020**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process

2020-FMIC-B-010 **March 25, 2020**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes

2020-MO-B-011 **March 25, 2020**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

The Board Can Improve Its Contract Administration Processes

2020-FMIC-B-012 **March 30, 2020**

Total number of recommendations: 13
Recommendations open: 13

See the summary in the body of this report.

Bureau of Consumer Financial Protection

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

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2013	1	1
2014	1	1
2015	0	0
2016	2	2
2017	1	2
2018	4	10
2019	5	20
2020[a]	1	3

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

a. Through March 31, 2020.

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

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

Total number of recommendations: 14
Recommendations open: 1

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

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

2014 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 3
Recommendations open: 1

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

The CFPB 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: 1

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

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

2016 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 3
Recommendations open: 1

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

We found that the Bureau had taken several steps to mature its information security program to ensure that it was consistent with FISMA requirements. For instance, we found that both the information

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

2017 Audit of the CFPB's Information Security Program

2017-IT-C-019 October 31, 2017

Total number of recommendations: 7
Recommendations open: 2

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: 2

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

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

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

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

Total number of recommendations: 2
Recommendations open: 1

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

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

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

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

Total number of recommendations: 4
Recommendations open: 4

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

2018 Audit of the Bureau's Information Security Program

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

Total number of recommendations: 4
Recommendations open: 3

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

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

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

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

Total number of recommendations: 6
Recommendations open: 4

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

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

Technical Testing Results for the Bureau's SQL Server Environment (nonpublic memorandum)

2019-IT-C-007R **May 22, 2019**

Total number of recommendations: 5
Recommendations open: 5

We identified that the security configurations for select SQL Server instances and databases were not aligned with established baselines and that significant weaknesses exist in controls for account management and configuration management. We believe that these continuing weaknesses heighten the risk of a breach of sensitive data maintained in the Bureau's SQL Server environment.

Bureau Efforts to Share Consumer Complaint Data Internally Are Generally Effective; Improvements Can Be Made to Enhance Training and Strengthen Access Approval

2019-FMIC-C-008 **June 3, 2019**

Total number of recommendations: 6
Recommendations open: 1

We examined (1) the extent to which the Office of Consumer Response's consumer complaint–sharing efforts help to inform the work of internal stakeholders and (2) Consumer Response's controls over internal access to shared complaint data, which can contain sensitive consumer information.

Overall, Consumer Response effectively shares consumer complaint data within the Bureau. To increase the incorporation of complaint data in the Bureau's work, Consumer Response can better educate users about the internal complaint-sharing tools and can enhance access controls to ensure that access to complaint data is limited to only users who need such information to perform their job functions.

The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP

2019-IT-C-009 **July 17, 2019**

Total number of recommendations: 3
Recommendations open: 3

To meet our FISMA requirements, we determined whether the Bureau has implemented an effective life cycle process for deploying and managing Federal Risk and Authorization Management Program (FedRAMP) cloud systems, including ensuring that effective security controls are implemented.

We found that the Bureau has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the FedRAMP cloud systems it uses. However, we found that the process is not yet effective in ensuring that (1) risks are comprehensively assessed prior to deploying new cloud systems, (2) continuous monitoring is performed to identify security control weaknesses after deployment, and (3) electronic media sanitization renders sensitive Bureau data unrecoverable when cloud systems are decommissioned.

2019 Audit of the Bureau's Information Security Program

2019-IT-C-015 **October 31, 2019**

Total number of recommendations: 7
Recommendations open: 7

See the summary in the body of this report.

The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed

2020-SR-C-002 **March 2, 2020**

Total number of recommendations: 3
Recommendations open: 3

See the summary in the body of this report.

Abbreviations

CBO	community banking organization
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
COR	contracting officer's representative
DATA Act	Digital Accountability and Transparency Act of 2014
DFMU	designated financial market utility
DLP	data loss protection
FedRAMP	Federal Risk and Authorization Management Program
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
IG	inspector general
IOC	Internal Oversight Committee
IT	information technology
LEU	Law Enforcement Unit
MDPS	multiregional data processing servicer
MRAs	Matters Requiring Attention
PIIA	Payment Integrity Information Act of 2019
PSU	Protective Services Unit
SEFL	Division of Supervision, Enforcement and Fair Lending
SR Letter 16-16	Supervision and Regulation Letter 16-16/Consumer Affairs Letter 16-7, *Special Post-Employment Restriction for Senior Examiners*

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