Office of Inspector General

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

Semiannual Report to Congress

April 1, 2019–September 30, 2019

OIG

Semiannual Report to Congress

April 1, 2019–September 30, 2019

Office of Inspector General

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

Message From the Inspector General

Each year, we list the major management challenges facing the Board of Governors of the Federal Reserve System (Board) and the Bureau of Consumer Financial Protection (Bureau)—in other words, the areas that, if not addressed, are most likely to impede the agencies' accomplishment of their strategic objectives. We recently issued the 2019 major management challenges, and one recurring theme is information security.

Information security is a growing concern for many of our stakeholders and for the federal government in general. In fact, October is National Cybersecurity Awareness Month. The Board Chairman has highlighted information security as one of the most significant risks facing the Board and financial institutions, and we have also heard concerns from congressional members about information security at the Board and the Bureau.

Information security is an area we have long been invested in and attuned to, as the Board and the Bureau both collect and store sensitive information as part of mission-critical work. Our Office of Information Technology conducts an annual audit of each agency to determine the effectiveness of their information security programs and reviews a subset of their information systems each year to determine compliance with their respective information security programs. We also have two information technology (IT) labs, where we conduct vulnerability scanning and where our Electronic Crimes Unit Special Agents recover deleted or hidden data. In addition, our staff members take extensive specialized training to stay up-to-date on the latest techniques and technology.

As part of our ongoing commitment to outreach, we also play an active role in the Office of Inspector General (OIG) community's efforts to improve information security. 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 Council of the Inspectors General on Integrity and Efficiency's Technology Committee.

Several of our recent reports concerning the Bureau's programs and operations focus on information security. The five Bureau reports we issued during the past 6 months examine the Bureau Civil Penalty Fund's compliance with the Improper Payments Information Act of 2002, as amended; security controls for SQL Server instances and databases; the Bureau's processes for sharing consumer complaint data internally; life cycle processes for the Federal Risk and Authorization Management Program, a

governmentwide program that assesses the safety of contractor-provided cloud services; and the Bureau's compliance with the Digital Accountability and Transparency Act of 2014.

We issued four reports on the Board's programs and operations. These reports cover the Board's government travel card program, workforce planning, internal processes for enforcement actions and terminations in the supervision of financial institutions, and internal processes for the Board Law Enforcement Unit's Operations Bureau. For these and for many other program areas at the Board, classifying and handling information in accordance with applicable information security requirements is a key tenet of operational effectiveness.

In the past 6 months, our Office of Investigations pursued cases involving abuse of authority, bank fraud, and other issues related to the programs and operations of the Board and the Bureau. We closed 17 investigations and processed 289 new hotline complaints. Our work resulted in 7 referrals for criminal prosecution; 1 indictment; 4 convictions; and over $387,000 in criminal fines, restitution, and special assessments. Electronic Crimes Unit Special Agents played a role in obtaining these results. Our investigative work continues to send a clear message that those who commit wrongdoing against the Board or the Bureau will be held accountable.

As technology advances, our methods evolve and the tools we use inevitably change. Nonetheless, our mission endures: providing independent oversight to improve programs and operations and to prevent and detect fraud, waste, and abuse. I know that we could not achieve this mission without our talented and dedicated staff, and I am deeply grateful every day for their steadfast commitment to excellence.

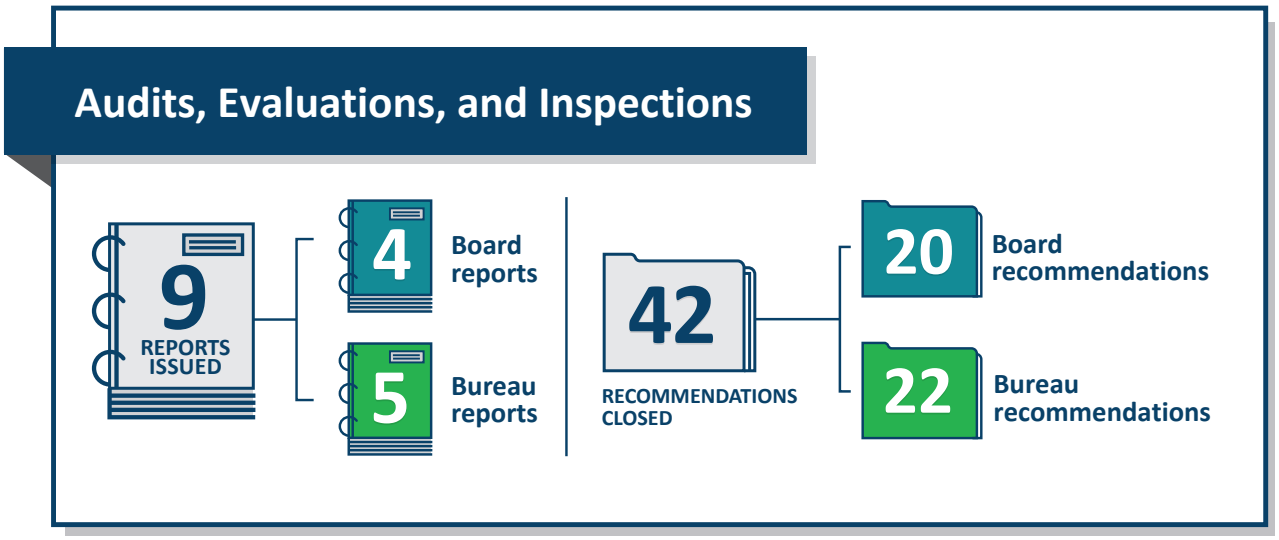
Sincerely,

Mark Bialek
Inspector General
October 31, 2019

Contents

Highlights

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



The Sharing of Consumer Complaint Data Within the Bureau

Overall, the Office of Consumer Response (Consumer Response) effectively shares consumer complaint data within the Bureau. Our review determined, however, that Consumer Response can better educate users about the internal complaint-sharing tools and can enhance access controls.

The Bureau's Life Cycle Processes for FedRAMP

The Bureau has developed a life cycle process for deploying and managing security risks for Bureau systems, which include the Federal Risk and Authorization Management Program (FedRAMP) cloud systems it uses. We found, however, that the process is not yet effective with respect to risk assessment, continuous monitoring, and electronic media sanitization.

Enterprise Workforce Planning at the Board

Although the Board has made initial progress in implementing enterprisewide workforce planning, we determined that 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 that may help the Board mitigate its operational challenges.

The Board's Enforcement Action Issuance and Termination Process

Supervision staff can use enforcement actions to compel a supervised institution's management to address safety and soundness or compliance issues identified through the supervisory process or other means. The Board and the Federal Reserve Banks have implemented some effective practices to support the processes for issuing and terminating enforcement actions against supervised institutions; however, we identified opportunities for the Board to enhance these processes.

Guilty Plea by Former First NBC Bank General Counsel in Conspiracy to Defraud the Bank

The former General Counsel of the failed First NBC Bank pleaded guilty to conspiracy to commit bank fraud. Along with others, he conspired to provide the bank with fraudulent documents that overstated the value of and understated liabilities of his personal and business assets. He faces up to 30 years in prison and a fine of more than $1 million.

Sentencing of Former Synovus Employee for Bank Fraud and Tax Evasion

A former commercial banker for Synovus Bank was sentenced to 24 months in federal prison after he pleaded guilty to four counts of bank fraud and four counts of tax evasion. While managing some of the bank's largest clients, he diverted over $1 million in client funds to a personal account at another bank. He was also ordered to pay restitution of nearly $400,000 to Synovus and the Internal Revenue Service.

Introduction

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

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

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

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

- Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act; 12 U.S.C. § 1831o(k)), 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 Improper Payments Information Act of 2002, as amended (IPIA; 31 U.S.C. § 3321 note), requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to IPIA. The Improper Payments Elimination and Recovery Act of 2010 requires us to determine each fiscal year whether the agency is in compliance with IPIA.
- Section 211(f) of the Dodd-Frank Act (12 U.S.C. § 5391(f)) requires that we review and report on the Board's supervision of any covered financial company that is placed into receivership. We are to evaluate the effectiveness of the Board's supervision, identify any acts or omissions by the Board that contributed to or could have prevented the company's receivership status, and recommend appropriate administrative or legislative action.
- Section 989E of the Dodd-Frank Act (5 U.S.C. app. 3 § 11 note) established the Council of Inspectors General on Financial Oversight (CIGFO), which is required to meet at least quarterly to share information and discuss the ongoing work of each Inspector General (IG), with a focus on concerns that may apply to the broader financial sector and ways to improve financial oversight.[1] Additionally, CIGFO must report annually about the IGs' concerns and recommendations, as well as issues that may apply to the broader financial sector. CIGFO can also convene a working group of its members to evaluate the effectiveness and internal operations of the Financial Stability Oversight Council, which was created by the Dodd-Frank Act and is charged with identifying threats to the nation's financial stability, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system.
- The Government Charge Card Abuse Prevention Act of 2012 (5 U.S.C. § 5701 note and 41 U.S.C. § 1909(d)) requires us to conduct periodic risk assessments and audits of the Bureau's purchase card, convenience check, and travel card programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments.
- Section 11B of the Federal Reserve Act (12 U.S.C. § 248(b)) mandates annual independent audits of the financial statements of each Federal Reserve Bank and of the Board. The Board performs the accounting function for the Federal Financial Institutions Examination Council (FFIEC), and we oversee the annual financial statement audits of the Board and of the FFIEC.[2] Under the Dodd-Frank Act, the U.S. Government Accountability Office performs the financial statement audit of the Bureau.

1. CIGFO comprises the IGs of the Board and the Bureau, the Commodity Futures Trading Commission, the U.S. Department of Housing and Urban Development, the U.S. Department of the Treasury, the Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, the 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 (Treasury) and the Office of Management and Budget (OMB). The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to the DATA Act and that only one specific DATA Act requirement, section 3(b), applies to the Bureau Fund. The DATA Act requires us to review a statistically valid sample of the data submitted by the agency and report on its completeness, timeliness, quality, and accuracy and on the agency's implementation and use of the data standards.

Major Management Challenges

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

In September 2019, we identified six major management challenges for the Board:

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

In September 2019, we identified three major management challenges for the Bureau:

- Ensuring That an Effective Information Security Program Is in Place
- Managing the Human Capital Program
- Continuing to Refine the Supervision and Enforcement Strategy

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

Audits, Evaluations, and Inspections

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

Evaluations and inspections include program evaluations and legislatively mandated reviews of failed financial institutions supervised by the Board. Evaluations are generally focused on the effectiveness of specific programs or functions. Inspections are often narrowly focused on particular issues or topics and provide time-critical analyses. Our evaluations and inspections are performed according to *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

Closure of the Audit of the Board's Fine Arts Program

May 8, 2019

The Board's Fine Arts Program acquires artwork through gifts and Board allocations related to major building renovations. Our objective was to assess the adequacy of internal controls related to the management and administration of the program, including the Board's process for acquiring artwork.

We found that the Fine Arts Program has controls in place that involve several Board divisions; these controls create a separation of duties that mitigates operational risk. Each division is aware of its responsibilities relating to Fine Arts Program processes. We also determined that the Fine Arts Program obtains the appropriate documentation and management approvals prior to acquiring artwork and monitors and tracks its artwork inventory.

Our scoping effort did not identify any potential internal control concerns that warranted further review.

Forensic Evaluation of the Board's Government Travel Card Program

2019-IT-B-010 **September 11, 2019**

The Board's government travel card (GTC) program provides employees with resources to arrange and pay for official travel and training-related expenses and to receive reimbursements for these authorized expenses. Through the U.S. General Services Administration's SmartPay program for government employees, the Board provides an individually billed charge card to each employee. The Board has issued its *Travel Policy* and *Government Travel Card Procedures*, which outline the requirements for using GTCs and detail the requirements of the travel program. Our objective was to identify potentially illegal, improper, or erroneous uses of GTCs during fiscal year 2018.

Overall, we did not find significant indicators of systemic fraud or illegal, improper, or erroneous use of GTCs. Based on the results of a series of 15 algorithms run on fiscal year 2018 travel program data, we conducted follow-up tests to determine whether there were exceptions, or indications of noncompliance with the Board's *Travel Policy* and *Government Travel Card Procedures*. We made observations based on six tests that resulted in exceptions; these observations related to reimbursement for lodging tax exemptions, reimbursement for hotel or meals and incidental expenses while on leave, reimbursement for overlapping vouchers on multicity trips, reimbursement for international travel, and charges for prohibited merchant category codes. Because we did not find any significant indicators of systemic fraud or any potentially illegal, improper, or erroneous use of GTCs, our report does not include formal recommendations.

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

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

Workforce planning is the systematic process for identifying and addressing the gaps between an organization's workforce of today and its future human capital needs. The Board's Human Resources (HR) function developed a preliminary enterprisewide workforce planning process in 2017 and began an initial pilot program with one division and one functional area of another division in 2018, which it has since completed. HR also developed a workforce plan with a third division and intends to complete a fourth workforce plan in 2019. 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. The Board has begun to address some of its challenges with these mitigating strategies; however, additional efforts to more comprehensively use these strategies may help the Board more timely implement and sustain an enterprisewide workforce planning process.

We also noted that HR should consider partnering with relevant divisions to coordinate workforce planning with other processes. By incorporating workforce planning into its existing administrative processes, such as strategic planning and enterprise risk management, the Board can help to ensure that it has centralized the workforce information necessary to make informed decisions when addressing operational priorities.

Our report contains recommendations to help the Board timely implement and sustain enterprisewide workforce planning. The Board concurred with our recommendations.

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**

The Board seeks to ensure that the financial institutions under its authority employ safe and sound business practices and comply with all applicable federal laws and regulations. If the Board or a Reserve Bank identifies significant concerns with these institutions through the supervisory process or other means, supervision staff can use enforcement actions to compel an institution's management to address the issues. 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.

Our report contains recommendations designed to enhance the efficiency and effectiveness of the Board's enforcement action issuance and termination processes. The Board concurred with our recommendations.

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

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

The mission of the Board's Law Enforcement Unit (LEU), which is part of the Management Division, is to provide a safe and secure environment for Board staff and others on Board-designated property. We assessed whether the control environment in the LEU's 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. The LEU is updating its current scheduling system; we did not evaluate the system revision because it was still under development at the end of our fieldwork.

Our report contains recommendations designed to improve internal processes associated with the Operations Bureau's control environment. The Board concurred with our recommendations.

Bureau of Consumer Financial Protection

Independent Accountants' Report on the Bureau Civil Penalty Fund's 2018 Compliance With the Improper Payments Information Act of 2002, as Amended

2019-FMIC-C-006 **April 29, 2019**

IPIA requires agency heads to periodically review and identify all programs and activities that may be susceptible to significant improper payments. We contracted with an independent public accounting firm to audit the Bureau Civil Penalty Fund's compliance with IPIA for fiscal year 2018. The contract required the audit to be performed in accordance with the auditing standards applicable to performance audits contained in *Government Auditing Standards*, which is issued by the Comptroller General of the United States. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with the contract and *Government Auditing Standards*.

The independent public accounting firm determined that the Bureau complied with the two applicable requirements of IPIA for fiscal year 2018 as they relate to the Civil Penalty Fund. Specifically, the firm found that the Bureau published an annual financial statement for the most recent fiscal year, posted that report on the agency website, and conducted a program-specific risk assessment in conformance with section 2(a) of IPIA. The other four IPIA requirements are not applicable to the Civil Penalty Fund because the Bureau has determined that the fund is not susceptible to significant improper payments. The firm made no recommendations in its report.

Technical Testing Results for the Bureau's SQL Server Environment

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

In a series of past reports, we have identified continuing weaknesses in security controls for select Bureau SQL Server instances and databases. Specifically, 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. Therefore, we issued this memorandum making recommendations to further assist the agency in its ongoing efforts to strengthen controls for its SQL Server instances and databases.

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**

Consumers have submitted over 1.7 million complaints about financial products and services with the Bureau since 2011. The effective sharing of complaint information among its divisions can help the Bureau understand the problems consumers are experiencing in the financial marketplace and identify and prevent unfair practices. We examined (1) the extent to which 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. Consumer Response can also enhance access controls to ensure that access to complaint data is limited to only users who need such information to perform their job functions.

Our report contains recommendations designed to further enhance the effectiveness of Consumer Response's internal complaint-sharing efforts and to strengthen access controls over complaint data containing sensitive consumer information. The Bureau concurred with our recommendations.

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

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

FedRAMP was established in 2011 to provide federal agencies with a cost-effective, risk-based approach for the adoption and use of cloud computing services. The Bureau uses five FedRAMP cloud systems to support various mission and business processes, and it plans to move to a cloud-only information technology (IT) infrastructure by 2022. To meet our FISMA requirements, we determined whether the Bureau has implemented an effective life cycle process for deploying and managing 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.

Our report contains recommendations designed to strengthen the Bureau's life cycle processes for leveraging FedRAMP cloud systems in the areas of risk management, continuous monitoring, and electronic media sanitization. The Bureau concurred with our recommendations.

Independent Accountants' Report on the Bureau's 2019 Compliance With the Digital Accountability and Transparency Act of 2014

2019-FMIC-C-011 **September 25, 2019**

The DATA Act aims to help policymakers and the public follow the flow of federal dollars by requiring agencies to submit certain spending data to USAspending.gov. We contracted with an independent public accounting firm to audit the Bureau's compliance with the act, and we reviewed and monitored the work to ensure compliance with the contract and *Government Auditing Standards*, which is issued by the Comptroller General of the United States. The audit assessed (1) the completeness, timeliness, accuracy, and quality of the Bureau's fiscal year 2019 first-quarter financial and award data submitted for publication on USAspending.gov and (2) the Bureau's implementation and use of the governmentwide financial data standards established by OMB and Treasury.

The independent public accounting firm found that the Bureau met DATA Act submission requirements. All data required to be published within the firm's sample were complete, timely, accurate, and of good quality. In addition, the firm found that the Bureau followed the applicable governmentwide financial data standards established by OMB and Treasury. The independent public accounting firm's report contains no 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 CIGIE's *Quality Standards for Investigations* and the *Attorney General Guidelines for Offices of Inspector General with Statutory Law Enforcement Authority*.

During this period, the Office of Investigations met with officials at both the Board and the Bureau to discuss investigative operations and the investigative process. The office also met with 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.

Former First NBC Bank General Counsel Pleaded Guilty in Conspiracy to Defraud the Bank

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

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

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

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

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

New Orleans Business Owner Charged and Pleaded Guilty to Conspiracy to Defraud First NBC Bank

A business owner who borrowed from First NBC Bank, a New Orleans–based bank that failed in April 2017, was charged with and pleaded guilty to conspiracy to commit bank fraud in the U.S. District Court for the Eastern District of Louisiana. The bank was a subsidiary of First NBC Bank Holding Company, a Board-supervised bank holding company.

The business owner, a bank President (the same as in the above case), and others knowingly conspired to defraud First NBC Bank. To secure loans they knew the business owner would be unable to repay, they provided materially false and fraudulent documents and financial statements that overstated the value of the business owner's assets, understated his liabilities, and omitted material information. The loans were falsely stated to be for business expenses but were actually used to pay for the business owner's personal expenses as well as overdrafts and payments from previous First NBC Bank loans, which made the new loans appear current and performing and the old loans appear paid. The business owner could face up to 30 years' imprisonment, a fine of more than $1 million or twice the gross gain to him or the gross loss of any victims, 5 years' supervised release, and a special assessment of $100.

This was a joint investigation by our office, the FBI, and the FDIC OIG and was prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

Former Synovus Employee Sentenced for Bank Fraud and Tax Evasion

A former commercial banker for Synovus Bank, a state member bank, was sentenced to 24 months in federal prison after he pleaded guilty to four counts of bank fraud and four counts of tax evasion. He was also ordered to pay restitution of $166,481 to Synovus and $221,357 to the Internal Revenue Service.

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

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

Bureau of Consumer Financial Protection

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

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

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

Other than the material found in appendix B, no publicly reportable developments occurred during this reporting period in our Bureau-related investigations.

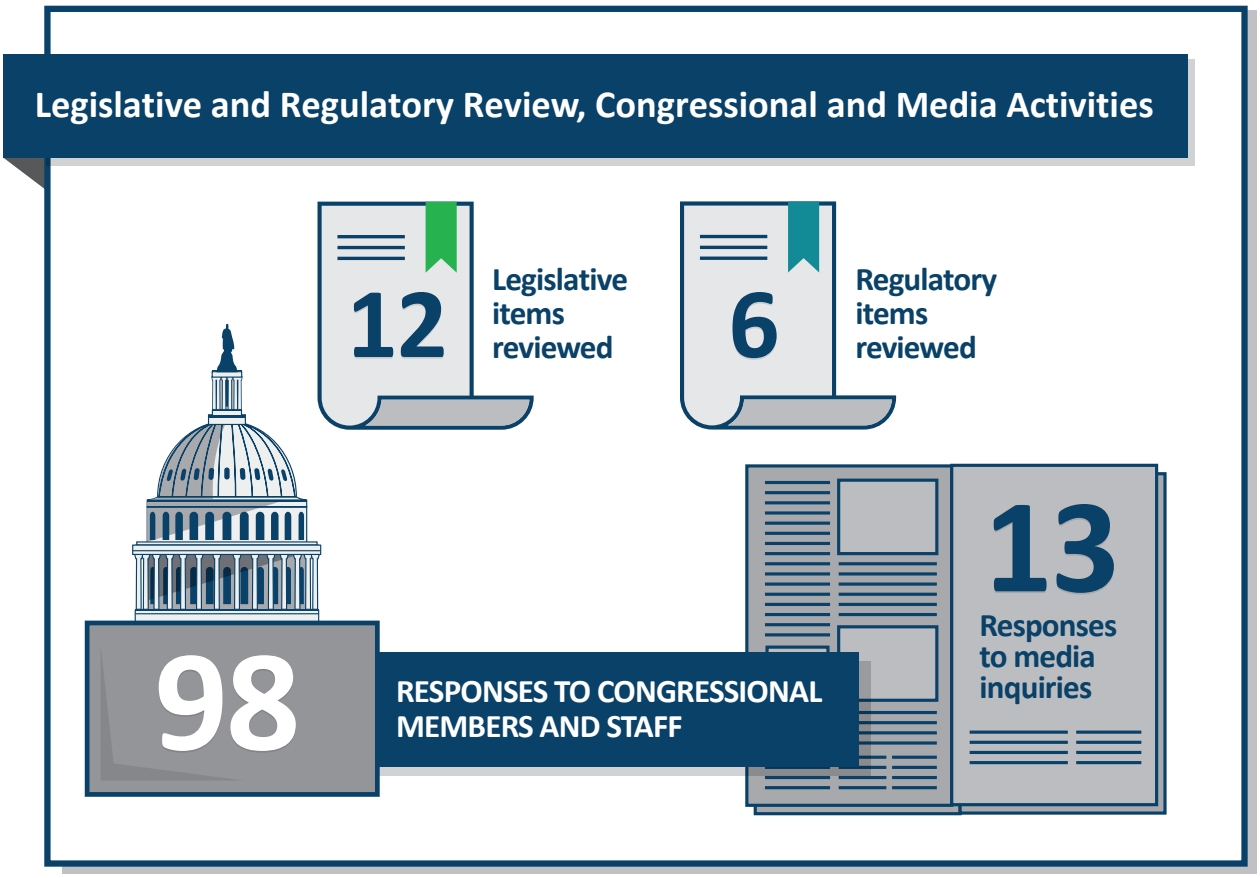
Hotline

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 289 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 (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 12 legislative items and 6 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 98 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 13 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 13,000 reports, detailing for fiscal year 2019 alone over $24 billion in potential savings and over 7,000 recommendations to improve programs across the federal government.

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

Our Associate Inspector General for Information Technology, as the Chair of the Information Technology Committee of the Federal Audit Executive Council, works with IT audit staff throughout the OIG community and reports to the CIGIE 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 June 2019, we led an inspection and evaluation peer review team, consisting of representatives from three OIGs, that reviewed the FDIC OIG. The review found that the FDIC OIG sufficiently met CIGIE standards and its internal policy and procedures.
- 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.

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
Forensic Evaluation of the Board's Government Travel Card Program	Evaluation
Leveraging Certain Strategies May Help the Board Timely Implement and Sustain Enterprisewide Workforce Planning	Evaluation
The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency	Evaluation
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	Evaluation
Total number of audit reports: 0 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	07/19	0	2
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	0	03/19	7	1
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	0	01/19	0	1
Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	07/14	3[a]	3	0	08/19	3	0
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle	12/14	3	3	0	10/18	2	1
Review of the Failure of Waccamaw Bank	03/15	5	5	0	08/19	3	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
Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)	09/15	3	3	0	06/19	3	0
Security Control Review of the Board's Active Directory Implementation (nonpublic report)	05/16	10	10	0	05/19	9	1
2016 Audit of the Board's Information Security Program	11/16	9	9	0	06/19	7	2
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	0	09/19	9	2
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing	04/17	8	8	0	08/19	4	4
2017 Audit of the Board's Information Security Program	10/17	9	9	0	06/19	2	7
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	09/19	7	7
Security Control Review of the RADAR Data Warehouse (nonpublic report)	03/18	3	3	0	n.a.	0	3

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
Security Control Review of the Board's Public Website (nonpublic report)	03/18	7	7	0	03/19	0	7
Knowledge Management for the Board's Comprehensive Liquidity Analysis and Review Is Generally Effective and Can Be Further Enhanced	09/18	3	3	0	08/19	3	0
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic report)	09/18	9	9	0	n.a.	0	9
2018 Audit of the Board's Information Security Program	10/18	6	6	0	06/19	0	6
Evaluation of the Board's Implementation of Splunk (nonpublic report)	11/18	1	1	0	n.a.	0	1
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	n.a.	1	5
The Board's Currency Shipment Process Is Generally Effective but Can Be Enhanced to Gain Efficiencies and to Improve Contract Administration	12/18	8	8	0	07/19	0	8
The Board Can Strengthen Controls Over Its Academic Assistance Program	12/18	9	9	0	07/19	0	9

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 Take Additional Steps to Advance Workforce Planning	03/19	2	2	0	08/19	0	2
Leveraging Certain Strategies May Help the Board Timely Implement and Sustain Enterprisewide Workforce Planning	09/19	2	2	0	n.a.	0	2
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	n.a	0	6
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	09/19	6	6	0	n.a.	0	6

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

n.a. not applicable.

a. These recommendations were directed jointly to the Office of the Comptroller of the Currency, the FDIC, and the Board.

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

Report title	Type of report
Independent Accountants' Report on the Bureau Civil Penalty Fund's 2018 Compliance With the Improper Payments Information Act of 2002, as Amended	Audit
Technical Testing Results for the Bureau's SQL Server Environment	Audit
Bureau Efforts to Share Consumer Complaint Data Internally Are Generally Effective; Improvements Can Be Made to Enhance Training and Strengthen Access Approval	Evaluation
The Bureau Can Improve the Effectiveness of Its Life Cycle Processes for FedRAMP	Evaluation
Independent Accountants' Report on the Bureau's 2019 Compliance With the Digital Accountability and Transparency Act of 2014	Audit
Total number of audit reports: 3 Total number of evaluation reports: 2	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity	09/13	14	14	0	03/19	13	1
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	06/19	2	1
The CFPB Can Enhance Its Diversity and Inclusion Efforts	03/15	17	17	0	08/19	17	0
The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	0	03/19	6	3
2016 Audit of the CFPB's Information Security Program	11/16	3	3	0	07/19	2	1
The CFPB Can Improve Its Examination Workpaper Documentation Practices	09/17	17	17	0	06/19	17	0
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	09/19	9	2
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	n.a.	0	2

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Bureau's Travel Card Program Controls Are Generally Effective but Could Be Further Strengthened	09/18	4	4	0	03/19	0	4
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	07/19	0	4
The Bureau Can Improve Its Follow-Up Process for Matters Requiring Attention at Supervised Institutions	01/19	6	6	0	n.a.	0	6
The Bureau Can Improve Its Risk Assessment Framework for Prioritizing and Scheduling Examination Activities	03/19	4	4	0	n.a.	1	3
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	09/19	1	5
The Bureau Can Improve The Effectiveness of Its Life Cycle Processes for FedRAMP	07/19	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	62
Investigations opened during the reporting period	13
Investigations closed during the reporting period	17
Investigations open at end of the reporting period	58
Investigative results for the reporting period	
Persons referred to U.S. Department of Justice prosecutors	7
Persons referred to state/local prosecutors	0
Declinations received	3
Joint investigations	36
Reports of investigation issued	3
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	3
Suspensions	0
Debarments	0
Prohibitions from banking industry	0
Indictments	1
Criminal informations	3
Criminal complaints	1
Convictions	4
Civil actions	$0
Administrative monetary recoveries and reimbursements	$0

See notes at end of table.

Investigative actions	Number or dollar value[a]
Civil judgments	$0
Criminal fines, restitution, and special assessments	$387,838
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	15
Complaints received during reporting period	289
Total complaints for reporting period	304
Complaints resolved during reporting period	269
Complaints pending	35

Appendix B: Inspector General Empowerment Act of 2016 Requirements

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

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

- We have no such instances to report.

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

- See appendix C.

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

- See table A-6.

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

- A former senior Bureau employee resigned following our investigation into an alleged misuse of his position. We found that the former senior Bureau employee created the appearance of a violation of the *Standards of Ethical Conduct for Employees of the Executive Branch* by using his position to request that his subordinate provide a statement in his support to the media. This matter was not presented to the U.S. Department of Justice because the associated allegations did not concern any department law enforcement interests, such as a potential violation of criminal law.

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.

- A former senior Bureau employee resigned following our investigation into an alleged misuse of his position. We found that the former senior Bureau employee created the appearance of a violation of the *Standards of Ethical Conduct for Employees of the Executive Branch* by using his position to request that his subordinate provide a statement in his support to the media. This matter was not presented to the U.S. Department of Justice because the associated allegations did not concern any department law enforcement interests, such as a potential violation of criminal law.

Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations

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

Board of Governors of the Federal Reserve System

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

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2011	1	2
2012	1	1
2013	1	1
2014	1	1
2015	1	2
2016	3	5
2017	3	18
2018	8	48
2019[a]	4	16

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

a. Through September 30, 2019.

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

June 13, 2011

Total number of recommendations: 2
Recommendations open: 2

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

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

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

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

March 30, 2012

Total number of recommendations: 8
Recommendations open: 1

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

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

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

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

Total number of recommendations: 1
Recommendations open: 1

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

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

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

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

Total number of recommendations: 3
Recommendations open: 1

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

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

Review of the Failure of Waccamaw Bank

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

Total number of recommendations: 5
Recommendations open: 2

In accordance with Dodd-Frank Act requirements, we concluded that Waccamaw Bank's failure presented unusual circumstances that warranted an in-depth review. Based on the in-depth review, we determined that Waccamaw Bank failed because its board of directors and senior management did not control the risks associated with the bank's rapid growth strategy. As a result, the bank sustained significant losses during a downturn in its local real estate market. In addition, we learned that (1) supervisory activity records were not retained in accordance with Board policy, (2) Waccamaw Bank's written agreement did not contain a provision that required regulatory approval of material transactions, and (3) Board and Federal Reserve Bank of Richmond appeals policies were silent on procedural aspects for second-level and third-level appeals.

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

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

Total number of recommendations: 10
Recommendations open: 1

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

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

2016 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 2

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

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

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

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

Total number of recommendations: 11
Recommendations open: 2

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

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

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

2017 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 7

We evaluated the effectiveness of the Board's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We followed U.S. Department of

Homeland Security guidelines and evaluated the information security program's maturity level (from a low of 1 to a high of 5) across several areas.

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

The Board's Organizational Governance System Can Be Strengthened

2017-FMIC-B-020 December 11, 2017

Total number of recommendations: 14
Recommendations open: 7

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

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

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

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

Total number of recommendations: 3
Recommendations open: 3

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

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

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

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

Total number of recommendations: 7
Recommendations open: 7

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

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

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

Total number of recommendations: 9
Recommendations open: 9

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

Overall, we found that the division has taken steps to implement information security controls for its general support system in accordance with FISMA and Board information security policies, procedures, standards, and guidelines. We identified opportunities for improvement in the implementation of the

Board's information system security life cycle for the division's general support system to ensure that information security controls are effectively implemented, assessed, authorized, and monitored.

2018 Audit of the Board's Information Security Program

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

Total number of recommendations: 6
Recommendations open: 6

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.

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

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

Total number of recommendations: 1
Recommendations open: 1

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

Overall, we found the Board implemented Splunk in line with security best practices. However, we identified an opportunity to strengthen risk management controls.

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: 9

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: 2

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 HR to divisions on HR's 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: 2

See the summary in the body of this report.

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: 6

See the summary in the body of this report.

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

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	4
2017	1	2
2018	4	12
2019[a]	5	22

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

a. Through September 30, 2019.

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

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

Total number of recommendations: 14
Recommendations open: 1

We determined the effectiveness of the Bureau's internal controls for its GTC program.

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

2014 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 3
Recommendations open: 1

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

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

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

Total number of recommendations: 9
Recommendations open: 3

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

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

2016 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 3
Recommendations open: 1

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

We found that the Bureau had taken several steps to mature its information security program to ensure that it was consistent with FISMA requirements. For instance, we found that both the information security continuous monitoring and incident response programs were operating at an overall maturity

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

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: 2

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

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

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

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

Total number of recommendations: 4
Recommendations open: 4

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

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

2018 Audit of the Bureau's Information Security Program

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

Total number of recommendations: 4
Recommendations open: 4

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: 6

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 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.

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

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

Total number of recommendations: 4
Recommendations open: 3

We assessed the effectiveness of SEFL's risk assessment framework, including the identification, analysis, and prioritization of specific institution product lines for examination, and we reviewed each region's implementation of the results of the prioritization process through examination scheduling.

We identified opportunities for the Bureau to improve its risk assessment framework for prioritizing and scheduling examinations. Specifically, SEFL's approach for assigning a key risk score to individual institution product lines is not transparent for some Bureau employees involved in the scoring process; these employees would benefit from additional training and guidance on that process. We also found that SEFL can improve its preliminary research on supervised institutions. Finally, we found that SEFL can improve the internal reporting of changes to the examination schedule.

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

See the summary in the body of this report.

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: 5

See the summary in the body of this report.

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

See the summary in the body of this report.

Abbreviations

Board	Board of Governors of the Federal Reserve System
Bureau	Bureau of Consumer Financial Protection
CFPB	Consumer Financial Protection Bureau
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
Consumer Response	Office of Consumer Response
DATA Act	Digital Accountability and Transparency Act of 2014
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FedRAMP	Federal Risk and Authorization Management Program
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
GTC	government travel card
HR	Human Resources
IG	Inspector General
IPIA	Improper Payments Information Act of 2002, as amended
IT	information technology
Legal Services	Office of Legal Services
LEU	Law Enforcement Unit
MDPS	multiregional data processing servicer
MRAs	Matters Requiring Attention
NRAS	National Remote Access Services
OIG	Office of Inspector General
OMB	Office of Management and Budget
RADAR	Risk Assessment, Data Analysis, and Research
SEFL	Division of Supervision, Enforcement and Fair Lending
Treasury	U.S. Department of the Treasury

Office of Inspector General
Board of Governors of the Federal Reserve System
Bureau of Consumer Financial Protection

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

OIG Hotline

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

800-827-3340