Office of Inspector General

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

Semiannual Report to Congress

October 1, 2020–March 31, 2021

OIG

Semiannual Report to Congress

October 1, 2020–March 31, 2021

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

Message From the Inspector General

Since our previous semiannual report to Congress, we have seen tremendous reason for hope with the approval and ongoing administration of several safe and effective vaccines for COVID-19. Still, the virus continues to claim hundreds of American lives every day, and thousands more are suffering economic effects from the pandemic.

We continue to actively monitor the Board of Governors of the Federal Reserve System's pandemic-related lending programs, including the design, operation, governance, and oversight of the programs; associated data collection and reporting; and the effect of the programs on the Board's supervision and regulation activities. In addition, our Office of Investigations is investigating numerous cases of pandemic-related fraud associated with loans worth tens of millions of dollars, including cases in which borrowers fraudulently applied for loans through pandemic response programs. Our work in this area sends a clear message that law enforcement is watching and will bring to justice those who seek to profit at the expense of those in need.

I also continue to serve on the Pandemic Response Accountability Committee (PRAC), which coordinates inspector general (IG) community oversight of the federal government's COVID-19 pandemic response efforts. The PRAC Financial Sector Workgroup recently organized a series of virtual listening panels with experts from the financial services sector—including the banking industry, borrower organizations, and housing experts—to obtain feedback and observations on the federal government's pandemic response programs from those with first-hand, on-the-ground experience. In January, along with the IG for the Federal Deposit Insurance Corporation, I moderated a listening panel focused on experiences from a cross-section of large, community, and minority-owned banks. The perspectives and observations of these stakeholders have been shared with PRAC member IGs, and a video of the panel is available on the PRAC website.

As vaccines become available, many people are eager to regain a sense of normalcy. But while we all look forward to reconnecting with our families, friends, and communities, it's not enough to aim for a return to normal. Over the past year, against the backdrop of a pandemic that has disproportionately affected Black, American Indian, Hispanic, and other minority Americans, our country has witnessed a surge of protests against long-standing systemic discrimination and racial injustice as well as an alarming rise in hate crimes and hostility against people of Asian and Pacific Islander descent.

Discrimination and racial injustice should have no place in our country or in our workplaces. Moreover, ensuring there are a wide range of perspectives in the workplace makes organizations more effective. In our recent report on the Bureau of Consumer Financial Protection's hiring practices, we find that the Bureau's overall workforce diversity increased from fiscal year 2014 to fiscal year 2019, and we identify six practices and supporting actions—many of which the Bureau is already following—for cultivating a diverse workforce.

Internally, we have also taken steps to support diversity within our organization. For example, our Diversity, Equity, and Inclusion Committee has hosted several listening events, hired a contractor to perform a cultural assessment, and distributed and discussed books about diversity and allyship. Diversity and inclusion is one of our core values and is at the center of our culture. I am committed to ensuring that our workplace is safe and inclusive for all our employees and that our workforce reflects the same diversity that makes our country vibrant and strong.

As we move forward, our workplaces themselves may also end up looking different than before. The Board is planning and managing major renovations of all four buildings it owns, and its long-term space planning strategy envisions the majority of employees working on a centralized Board campus. We examined the Board's management of its renovation projects in a report issued in this reporting period, and we also identified ensuring that physical infrastructure effectively meets mission needs as a major management challenge for the Board in 2021.

We continue to be concerned about information security. We again identified information security as a major management challenge for both the Board and the Bureau for 2021, and we are evaluating the Board's adoption of cloud computing systems. In addition, in January, our deputy inspector general participated as a panelist in a virtual cybersecurity roundtable hosted by minority members of the House Financial Services Committee.

We have also welcomed new leadership to both of the agencies we oversee. Dave Uejio was named acting director of the Bureau, and Christopher J. Waller took office as a member of the Board. We've met with Acting Director Uejio and Governor Waller, and we look forward to continuing to work with leadership at the Board and the Bureau as we provide independent oversight to improve their programs and operations and to prevent and detect fraud, waste, and abuse.

Finally, I'd like to thank my staff for their extraordinary efforts over the past year. The pandemic has required staff not only to take on new oversight responsibilities, but also to learn new technology and adapt to working remotely, often while balancing competing caregiving responsibilities. I am incredibly proud of the dedication, flexibility, and tremendous professionalism my staff have shown. I also want

to specifically recognize our special agents, who have continued to work in the field despite increased personal risk. The significant personal contributions my staff have made to ensure that we continue to accomplish our mission through these challenging times are truly a testament to their talent, dedication, and unwavering commitment.

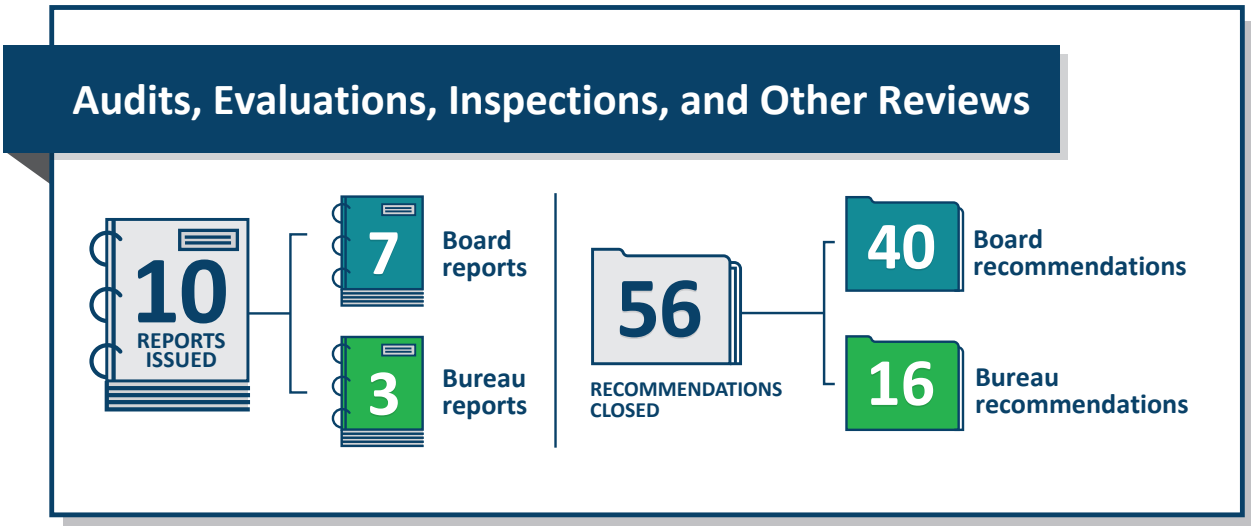
Sincerely,

Mark Bialek
Inspector General
April 30, 2021

Contents

Highlights

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



The Board's Information Security Program

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

The Board Economics Divisions' Planning Processes for Economic Analysis

The Board's four economics divisions—the Divisions of Research and Statistics, Monetary Affairs, International Finance, and Financial Stability—can enhance some of their planning processes for their economic analysis activities.

The Board's Management of Renovation Projects

The Board can improve its planning and management of ongoing renovation projects; these improvements can inform the planning and management of future large, complex, multidivision initiatives.

The Bureau's Information Security Program

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

The Bureau's Hiring Practices and Workforce Diversity

The Bureau can strengthen its hiring processes and reduce risks associated with certain of its hiring practices. The agency's racial and ethnic diversity increased as a percentage of its overall workforce from fiscal year 2014 to fiscal year 2019.

Former Executive of First NBC Bank Indicted for Bank Fraud and False Statements

A former senior vice president of First NBC Bank—the $5 billion New Orleans–based bank that failed in April 2017—was named in a superseding indictment for their role in an alleged fraud scheme totaling hundreds of millions of dollars and involving at least seven coconspirators. The defendant joins three other former First NBC Bank executives and a borrower named in the original indictment. The five defendants could face, for each of the dozens of charged counts, up to 30 years in prison, a fine of $1 million or the greater of twice the gain to a defendant or twice the loss to any victim, and up to 5 years' supervised release.

Former Bank Chief Executive Officer Sentenced to Prison for Falsifying Bank Records and Misappropriating More Than $1.6 Million

The former chief executive officer (CEO) of Border State Bank in Greenbush, Minnesota, was sentenced to 18 months in prison for making a false entry in bank records. The former CEO issued three unauthorized Standby Letters of Credit worth $1.6 million to facilitate the purchase and delivery of diamonds and gold from Africa, but did not report the letters to bank personnel, who would have logged them into the bank's general ledger where they could be tracked by regulators.

Former Whitaker Bank President Sentenced for Embezzlement

The former president of Whitaker Bank, a state member bank in Kentucky, was sentenced to 1 year and 1 day in prison after pleading guilty to embezzling or misapplying more than $50,000 of the bank's funds. The former president admitted to stealing property from a foreclosed country club and seeking reimbursement from the bank for personal expenses.

Business Owners Indicted for $7 Million Paycheck Protection Program Fraud

Two siblings were indicted and charged in New York with wire fraud conspiracy, bank fraud conspiracy, bank fraud, and engaging in monetary transactions with criminally derived property for their alleged participation in a scheme to file fraudulent Paycheck Protection Program (PPP) loan applications seeking nearly $7 million. They made numerous false and misleading statements about their companies' respective business operations and payroll expenses. To date, the government has seized over $400,000 of the more than $600,000 that the defendants obtained.

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.

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 15010 of the Coronavirus Aid, Relief, and Economic Security Act (CARES Act; 15 U.S.C. § 9001 note) established the Pandemic Response Accountability Committee (PRAC) within the Council of the Inspectors General on Integrity and Efficiency (CIGIE). PRAC is required to conduct and coordinate oversight of covered funds and the coronavirus response in order to detect and prevent fraud, waste, abuse, and mismanagement and identify major risks that cut across programs and agency boundaries. PRAC is also required to submit reports related to its oversight work to relevant federal agencies, the president, and appropriate congressional committees. The chairperson of CIGIE named our inspector general (IG) as a member of PRAC, and as such, we participate in PRAC meetings, conduct PRAC oversight activities, and contribute to PRAC reporting responsibilities.
- 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.

- 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.[1] Under the Dodd-Frank Wall Street Reform and Consumer Protection Act, the U.S. Government Accountability Office performs the financial statement audit of the Bureau.
- The Digital Accountability and Transparency Act of 2014 (DATA Act; 31 U.S.C. § 6101 note) requires agencies to report financial and payment data in accordance with data standards established by the U.S. Department of the Treasury and the Office of Management and Budget. The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to the DATA Act and that only one specific DATA Act requirement, section 3(b), applies to the Bureau Fund. The DATA Act requires us to review a statistically valid sample of the data submitted by the agency and report on its completeness, timeliness, quality, and accuracy and on the agency's implementation and use of the data standards.
- The Payment Integrity Information Act of 2019 (PIIA; 31 U.S.C. §§ 3351–58) requires agency heads to periodically review and identify programs and activities that may be susceptible to significant improper payments. The Bureau has determined that its Consumer Financial Civil Penalty Fund is subject to the PIIA. The PIIA requires us to determine each fiscal year whether the agency complies with the act.
- The Government Charge Card Abuse Prevention Act of 2012 (5 U.S.C. § 5701 note and 41 U.S.C. § 1909(d)) requires us to conduct periodic risk assessments and audits of the Board's and the Bureau's purchase card, convenience check, and travel card programs to identify and analyze risks of illegal, improper, or erroneous purchases and payments.
- Section 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 IG, with a focus on concerns that may

1. 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.

apply to the broader financial sector and ways to improve financial oversight.[2] 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.

- Section 38(k) of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act (12 U.S.C. § 1831o(k)), outlines certain review and reporting obligations for our office when a state member bank failure occurs. The nature of those review and reporting requirements depends on the size of the loss to the Deposit Insurance Fund.
- The Federal Reserve Act, as amended by the USA PATRIOT Act of 2001 (12 U.S.C. § 248(q)), grants the Board certain federal law enforcement authorities. We perform the external oversight function for the Board's law enforcement program.

2. 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.

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 March 2021, we identified seven major management challenges for the Board:

- Designing and Operationalizing Emergency Lending Programs to Address the Economic Effects of the COVID-19 Pandemic
- Enhancing Organizational Governance and Risk Management
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Ensuring an Effective Information Security Program
- Strengthening the Human Capital Program and Ensuring Workforce Safety
- Remaining Adaptable to External Developments While Supervising Financial Institutions
- Ensuring That Physical Infrastructure Effectively Meets Mission Needs

In March 2021, we identified four major management challenges for the Bureau:

- Ensuring That an Effective Information Security Program Is in Place
- Managing Human Capital and Ensuring Employee Safety
- Remaining Adaptable to External Developments While Continuing to Refine the Supervision and Enforcement Strategy
- Managing Consumer Complaints

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

Audits, Evaluations, Inspections, and Other Reviews

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

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

Other reviews may include risk assessments, data analytics or other testing, and program and operational reviews that may not be performed in accordance with audit or evaluation standards.

The information below summarizes our audits, evaluations, and other reviews completed during the reporting period.

Board of Governors of the Federal Reserve System

2020 Audit of the Board's Information Security Program

2020-IT-B-020 **November 2, 2020**

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 continues to operate effectively at a level-4 (*managed and measurable*) maturity. The Board has opportunities to mature its information security program in FISMA

domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

Similar to our previous FISMA audits, a consistent theme we noted is that the decentralization of information technology (IT) services results in an incomplete view of the risks affecting the Board's security posture. In addition, the Board has not completed defining its enterprisewide risk management strategy, risk appetite, and risk tolerance levels; defining them could help guide cybersecurity processes across function areas. We also believe that the Board's ongoing efforts to implement the U.S. Department of Homeland Security's Continuous Diagnostic and Mitigation program will continue to mature the agency's information security program across multiple security functions and help address issues that result from the decentralization of IT services.

The Board has taken sufficient action to close 7 of the 18 recommendations from our prior FISMA audits that remained open at the start of this audit. This report contains 4 new recommendations and 2 matters for management consideration designed to strengthen the Board's information security program in the areas of risk management, configuration management, identity and access management, data protection and privacy, and information security continuous monitoring. The Board concurred with our recommendations.

Calendar Year 2019 Risk Assessment of the Board's Government Travel Card Program

February 22, 2021

Board travel cards were used for 26,149 transactions totaling some $9.8 million in 2019. We conducted a risk assessment of the Board's travel card program to determine the necessary frequency and scope of travel card audits. The results of our assessment show that the risk of illegal, improper, or erroneous use in the Board's travel card program is *low*. A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would be expected to have a minimal effect on current operations and long-term objectives. Nonetheless, the Board's Travel section should continue to take appropriate actions to ensure proper oversight of its program. As a result of the low risk level, we will not include an audit of the Board's government travel card program in our 2021 audit plan.

Calendar Year 2019 Risk Assessment of the Board's Purchase Card Program

February 22, 2021

Board purchase cards were used for about $2.8 million in total program spending in 2019. We conducted a risk assessment of the Board's purchase card program to determine the necessary frequency and scope of purchase card audits. The results of our assessment show that the risk of illegal, improper, or

erroneous use in the Board's purchase card program is *low*. A risk level of *low* means that illegal, improper, or erroneous use is unlikely to occur and that such an occurrence would be expected to have a minimal effect on current operations and long-term objectives. Nonetheless, the Board's Purchase Card section should continue to take appropriate actions to ensure proper oversight of its program. As a result of the low risk level, we will not include an audit of the Board's purchase card program in our 2021 audit plan.

The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis

2021-MO-B-001 **February 24, 2021**

The Board's four economics divisions—the Divisions of Research and Statistics, Monetary Affairs, International Finance, and Financial Stability—produce analysis and research to support the Board's mission. The economics divisions use a variety of processes and supporting practices to plan such analysis. We assessed the economics divisions' processes to plan certain research activities and identified opportunities to enhance the effectiveness of those processes.

We found that the economics divisions can enhance some of their planning processes for their economic analysis activities by considering additional practices to improve transparency, communication, and monitoring. In addition, the economics divisions' continuous improvement efforts can benefit from a more structured approach to sharing processes and supporting practices with each other.

We made recommendations designed to improve some of the economics divisions' planning processes. The Board concurred with our recommendations.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2020 and 2019, and Independent Auditors' Report

2021-FMIC-B-003 **February 25, 2021**

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

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the FFIEC as of December 31, 2020 and 2019, and the results of operations and cash flows for

the years then ended in conformity with accounting principles generally accepted in the United States. The auditors' report on internal control over financial reporting and on compliance and other matters disclosed no instances of noncompliance or other matters.

The Board Can Improve the Management of Its Renovation Projects

2021-FMIC-B-004 **March 10, 2021**

The Board is planning and managing major renovations of all four of the buildings it owns. The Board's total renovation budget, as of June 2020, was $2.1 billion. Leading project management practices for capital projects suggest that comprehensive planning, which includes project governance, provides a foundation for effectively managing that project. We assessed the Board's process for planning and managing multiple renovation projects as well as procuring services under various renovation-related contracts.

The Board's Facility Services section completed certain planning studies for the Marriner S. Eccles Building/1951 Constitution Avenue NW building renovation project and established clear roles and responsibilities for senior leadership with respect to managing changes to existing contracts. However, the section did not establish project governance before awarding the architectural and engineering contract for Eccles/1951. In addition, although Facility Services ensured that the contractors on the William McChesney Martin, Jr., Building renovation project submitted monthly progress reports, it did not ensure that the architectural and engineering firm for the Eccles/1951 renovation project submitted monthly progress reports or biweekly status meeting minutes as required by the contract. Additionally, Facility Services did not formally approve project schedule changes as required by the contract. Lastly, we found that the Board's policies and procedures aligned with industry and government practices for conducting market research and awarding competitive contracts to bidders and that the Board's market research and contract award activities complied with its policies and procedures.

Our report contains recommendations designed to further enhance the Board's planning and management of ongoing renovation projects as well as future large, complex, multidivision initiatives. The Board concurred with our recommendations.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2020 and 2019, and Independent Auditors' Report

2021-FMIC-B-005 **March 10, 2021**

We contracted with an independent public accounting firm to audit the financial statements of the Board and to audit the Board's internal control over financial reporting. The contract requires the audits of the

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

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2020 and 2019, and the results of its operations and its cash flows for the years then ended in conformity with accounting principles generally accepted in the United States. Also, in the auditors' opinion, the Board maintained, in all material respects, effective internal control over financial reporting as of December 31, 2020, based on the criteria established in *Internal Control—Integrated Framework* (2013) by the Committee of Sponsoring Organizations of the Treadway Commission. The auditors' report on compliance and other matters disclosed no instances of noncompliance or other matters.

Bureau of Consumer Financial Protection

2020 Audit of the Bureau's Information Security Program

2020-IT-C-021 November 2, 2020

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 continues to operate effectively at a level-4 (*managed and measurable*) maturity.

Similar to our previous FISMA audits, we identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective. This year, we identified policy and technology improvements needed to strengthen separation of duties controls in the Bureau's configuration management processes.

The Bureau has taken sufficient actions to close 4 of the 14 recommendations from our prior FISMA audits that were open at the start of this audit. This report includes 1 new recommendation designed

to strengthen the Bureau's information security program in the area of configuration management. The Bureau concurred with our recommendation.

Forensic Evaluation of the Bureau's Vendor Payment Process

2021-IT-C-002 **February 24, 2021**

The Bureau maintains an interagency agreement with the U.S. Department of the Treasury's Bureau of the Fiscal Service, Administrative Resource Center to award contracts for various goods and services on behalf of the Bureau. From January 1, 2018, through June 30, 2019, the Bureau made payments on invoices totaling about $300 million. We conducted a forensic evaluation to identify potentially illegal, improper, or erroneous transactions or activities in the vendor payment process.

Overall, we did not find significant indicators of potentially illegal, improper, or erroneous transactions or activities in the Bureau's vendor payment process. Our report does not contain formal recommendations.

The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce

2021-MO-C-006 **March 29, 2021**

As an executive agency, the Bureau can fill positions by using competitive hiring authorities as well as hiring authorities that are specifically excepted from the competitive service. To guide its hiring practices, the Bureau's Office of Human Capital has eight policy, standard operating procedure, and guidance documents related to its hiring processes. We assessed the Bureau's compliance with its policies and procedures related to selected types of hiring, promotions, and other internal placements and to identify any potential effects of those hiring practices on its workforce diversity.

We found that the Bureau did not consistently conduct structured interviews or follow its planned assessment process regarding the use of structured interviews. In addition, the Bureau's policy and procedure documents did not provide guidance to hiring managers outlining expectations for (1) documenting qualified internal applicants for inclusion in interviews or (2) selecting interview panels.

We also found that the Bureau generally follows its policy, procedure, and guidance requirements for the hiring processes we examined. However, certain practices differed from those established in its policy, procedure, and guidance documents for controls surrounding public disclosure of one type of its excepted service positions and the use of subject-matter experts. In addition, the Bureau did not consistently document justifications for selecting an applicant or using subject-matter experts for the hiring actions that we tested. Further, we identified updates to hiring action documentation that occurred months after the position was filled. Finally, we found that the Bureau's database for tracking hiring actions has

incomplete data and lacks system controls to ensure data reliability. Specifically, we identified that six of eight key date fields in the tracking database were frequently blank.

We found that the Bureau's racial and ethnic diversity increased as a percentage of its overall workforce from fiscal year 2014 to fiscal year 2019. We identified six practices and supporting actions for cultivating a diverse workforce and found that although the Bureau's hiring processes aligned with many of these practices and supporting actions, several practices may help the Bureau continue to increase its workforce diversity.

We made recommendations designed to strengthen the Bureau's hiring processes and reduce risks associated with certain of its hiring practices and a recommendation to help the Bureau maintain its focus on hiring a diverse workforce. The Bureau concurred with our 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.

Investigations

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

During this period, the Office of Investigations met with officials at both the Board and the Bureau to discuss investigative operations and the investigative process. The office also met with counterparts at other financial regulatory agency offices of inspector general 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 Crown Bank CEO Sentenced to Prison for Fraud

The former CEO of Crown Bank in Minnesota was sentenced to 1 year and 1 day in prison, followed by 2 years' supervised release, after pleading guilty to one count of wire fraud and one count of filing a false income tax return. The former CEO was also ordered to pay $190,500 restitution and a $200 special

assessment and cannot hold employment with fiduciary responsibilities without prior approval from the probation office. Crown Bank is a subsidiary of Crown Bankshares Inc., a Board-supervised bank holding company for which the offender also served as president and member of the board of directors.

The former CEO fraudulently used the bank's funds to pay substantial personal debts and expenses and altered records to hide their activity. From 2012 to 2017, the former CEO made false entries to conduct transactions for their own benefit without notifying the bank's board of directors and without properly notifying the appropriate state and federal regulatory agencies. The former CEO also deceived investors about a pending deal for another bank to acquire Crown Bank at a premium when there was no agreement with the bank in question. Further, the former CEO filed a false income tax return for 2016 by not disclosing $720,000 in income from transactions designed to look like loans or stock purchases from third parties but that were instead going directly to themself. The false tax return resulted in a tax loss of about $285,200.

This case was investigated by our office, the Federal Bureau of Investigation (FBI), the Federal Deposit Insurance Corporation (FDIC) OIG, and the Internal Revenue Service (IRS) Criminal Investigation (CI). It was prosecuted by the U.S. Attorney's Office for the District of Minnesota in Minneapolis.

Former Bank CEO Sentenced to Prison for Falsifying Bank Records and Misappropriating More Than $1.6 Million

The former CEO of Border State Bank in Greenbush, Minnesota, was sentenced to 18 months in prison for making a false entry in bank records. The former CEO served as a director of the bank's holding company, Border Bancshares Inc., which is supervised by the Board, and held various executive positions in other banks that Border Bancshares Inc. acquired, including the former First State Bank of Clearbrook and the former First Advantage Bank.

In late 2015 and early 2016, the former CEO loaned money to a bank customer to invest in a diamond and gold venture in Liberia, Ghana, and Kenya that promised a quick return. After depleting their personal funds on the investment and exhausting the amount they could borrow from the bank, the former CEO asked other individuals, including bank customers, shareholders, and directors of the bank, to lend them money to recover the former CEO's personal funds. In 2016 and 2017, the former CEO requested a series of loans by having bank customers take out loans in their names or draw from loans they already had before the former CEO transferred the funds to themself. In May 2016, the former CEO issued and signed as CEO three unauthorized Standby Letters of Credit (SBLCs) worth $1.6 million on First Advantage Bank letterhead to facilitate the purchase and delivery of diamonds and gold from Africa. SBLCs are considered obligations of a bank and can affect a bank's financial standing. The former CEO concealed these actions by failing to report the SBLCs to bank personnel, who would have logged them into the bank's general

ledger where the SBLCs could be tracked by regulators. The offender abused their position as CEO and put the bank and its customers at risk.

This case was investigated by our office, the FBI, and the FDIC OIG. It was prosecuted by the U.S. Attorney's Office for the District of Minnesota in Minneapolis.

Former Whitaker Bank President Sentenced for Embezzlement

The former president of Whitaker Bank, a state member bank in Kentucky, was sentenced to 1 year and 1 day in prison after pleading guilty to embezzling or misapplying more than $50,000 of the bank's funds.

The former president admitted to willfully misapplying assets of the bank from January 12, 2016, to August 13, 2018. The former president admitted to stealing golf carts and other property from a foreclosed country club owned by Whitaker Bank and admitted to being reimbursed for personal expenses, including vehicle repairs, technology purchases for family members, and residential landscaping, which the former president intentionally misreported as legitimate work expenses.

This case was investigated by our office, the FBI, and the FDIC OIG. It was prosecuted by the U.S. Attorney's Office for the Eastern District of Kentucky.

Former Executive of First NBC Bank Indicted for Bank Fraud and False Statements

A former senior vice president of First NBC Bank was named in a superseding indictment for defrauding the $5 billion New Orleans–based bank that failed in April 2017. This individual joined three other former First NBC Bank executives and a borrower named in the original indictment, which we reported in our previous semiannual report to Congress. If convicted, the five defendants face, for each of the dozens of charged counts, up to 30 years in prison, a fine of $1 million or the greater of twice the gain to a defendant or twice the loss to any victim, up to 5 years' supervised release, and a $100 mandatory special assessment.

From 2006 through April 2017, the defendants allegedly conspired to defraud First NBC Bank through a variety of schemes. Specifically, they conspired with others to defraud the bank by disguising the financial status of certain borrowers and their troubled loans, concealing the true financial condition of the bank from the board, auditors, and examiners.

During the course of the conspiracy, the executives repeatedly extended new loans to borrowers to cover their previous loans and overdraft fees, which they could not have otherwise paid. To hide this practice, the executives made false statements in loan documents and elsewhere about the purposes of the loans, the borrowers' abilities to repay the loans, and the sources of funds used to pay the loans. The new loans

also prevented the borrowers from appearing on lists that the executives gave the bank's board each month, which would have highlighted that the borrowers were unable to make loan payments or had cash flow problems. When members of the board or the bank's outside auditors or examiners asked about loans to these borrowers, the executives made further false statements to conceal their activities.

As a result, the balance on these borrowers' loans continued to grow, even as the executives each received millions in compensation. By the time regulators closed First NBC Bank in April 2017, the borrowers owed more than $250 million. The bank's failure cost the FDIC's Deposit Insurance Fund just under $1 billion.

This case was investigated by our office, the FBI, and the FDIC OIG. It is being prosecuted by the U.S. Attorney's Office for the Eastern District of Louisiana.

Florida Individual Pleaded Guilty in $3.9 Million PPP Investigation

A Florida individual pleaded guilty to one count of wire fraud after fraudulently obtaining some $3.9 million in PPP loans and using those funds, in part, to buy a $318,000 Lamborghini. PPP loans are forgivable and guaranteed by the U.S. Small Business Administration (SBA) under the CARES Act. Authorities seized $3.4 million from the defendant's bank accounts and the car at the time of their arrest.

The defendant admitted to fraudulently seeking millions of dollars in PPP loans through applications to an insured financial institution on behalf of different companies. The applications made numerous false and misleading statements about the companies' respective payroll expenses. The financial institution approved and funded about $3.9 million in loans. Within days of receiving the PPP funds, the defendant purchased a 2020 Lamborghini Huracán, which they registered jointly in their name and in the name of one of their companies. Soon after, the defendant failed to make the payroll payments they claimed on their loan applications. The defendant did, however, make purchases at luxury retailers and resorts in Miami Beach.

This case was investigated by our office, the FDIC OIG, the IRS CI, the SBA OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the U.S. Department of Justice (DOJ) and the U.S. Attorney's Office for the Southern District of Florida.

Oklahoma Individual Pleaded Guilty to PPP Fraud

An Oklahoma individual pleaded guilty to bank fraud in a scheme to defraud the First Bank of Owasso by applying for a PPP loan under false pretenses. As part of the plea, the defendant agreed to a sentence of 12 months and 1 day in prison and restitution of $97,800 to be paid to First Bank of Owasso. Sentencing will occur at a later date.

The defendant applied for a PPP loan on behalf of Maturino Enterprises Inc., a company they claimed to own and operate. The defendant submitted forms that misrepresented the company's payroll spending, number of employees, and taxes paid. The defendant also admitted to misrepresenting how the loan would be used, saying that they would use the loan funds to retain workers and maintain payroll or make mortgage interest, lease, and utility payments in accordance with PPP rules.

This case was investigated by our office, the FBI, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Oklahoma Individual Charged With Fraudulently Applying for PPP Loans

An Oklahoma individual was charged with aggravated identity theft in a scheme to defraud Regent Bank when applying for a PPP loan.

The defendant applied for a PPP loan on behalf of Velocity Innovations LLC, a company they claimed to own and operate. As part of the application, the defendant used the identities of at least seven people without their knowledge, fraudulently claiming that those individuals were employees of Velocity Innovations LLC. The defendant received $125,900 from the bank as a result the scheme.

This case was investigated by our office, the FBI, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Four Individuals Charged in Attempted $5.4 Million PPP Fraud

Four individuals in Oklahoma are facing 22 charges, including bank fraud conspiracy, bank fraud, aggravated identity theft, money laundering, and false statements, for allegedly conspiring to fraudulently obtain over $5.4 million in PPP loans.

Three of the defendants created 12 fictitious business entities to fraudulently apply for about 22 PPP loans under false pretenses, such as payroll spending, number of employees, taxes paid, details of business ownership, and their relationships with one another. All four defendants submitted multiple applications for the same businesses to more than 12 banks without disclosing to those banks that they were submitting duplicative applications. They conspired to obtain over $5.4 million in loans and received close to $1 million from the banks.

This case was investigated by our office, the FBI, and the SBA OIG. It is being prosecuted by the U.S. Attorney's Office for the Northern District of Oklahoma.

Business Owners Indicted for $7 Million PPP Fraud

Two siblings, owners of multiple businesses, were indicted and charged in New York with wire fraud conspiracy, bank fraud conspiracy, bank fraud, and engaging in monetary transactions with criminally derived property for their alleged participation in a scheme to file fraudulent PPP loan applications seeking nearly $7 million.

According to the allegations, the siblings conspired to submit and submitted at least eight fraudulent PPP loan applications. In support of their applications, they made numerous false and misleading statements about their companies' respective business operations and payroll expenses. Further, the fraudulent loan applications were supported by fake documents, including falsified federal tax filings. Finally, the defendants used fraudulently obtained loan proceeds on personal expenses, including securities, home improvements, and a vehicle. To date, the government has seized over $400,000 of the more than $600,000 that the defendants obtained.

This case was investigated by our office, the FBI, the FDIC OIG, the Federal Housing Finance Agency OIG, and the SBA OIG. It is being prosecuted by the DOJ and the U.S. Attorney's Office for the Western District of New York.

New Jersey Businessperson Charged With $1.8 Million PPP Fraud

A New Jersey businessperson was charged with wire fraud, bank fraud, and money laundering for their alleged participation in a scheme to file fraudulent PPP loan applications. The individual was approved for three loans and received about $1.8 million in funding.

According to the allegations, the individual used multiple false statements regarding employees and average monthly payroll. The three PPP loan applications were submitted on behalf of three businesses. Once the PPP funds were received, the defendant diverted funds to various accounts belonging to their relatives, their minor children, and other businesses.

This case was investigated by our office, the FDIC OIG, IRS CI, SBA OIG, the U.S. Social Security Administration OIG, and the U.S. Postal Inspection Service. It is being prosecuted by the DOJ and the U.S. Attorney's Office for the District of New Jersey.

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 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.

Costa Rican Citizen Indicted for Fraudulent Lottery Scheme and False Statements

A citizen of Costa Rica living in El Paso, Texas, was indicted in connection with a lottery scheme to steal over $1 million from dozens of unsuspecting individuals. The defendant was charged with 1 count each of conspiracy to commit wire fraud, making a false statement to obtain credit, and conspiracy to commit money laundering and 10 counts of wire fraud. The United States is seeking forfeiture of the proceeds derived from the scheme as well as a money judgment of over $1.2 million against the defendant.

The defendant allegedly participated in or caused a series of fraudulent wire transfers in which victims, believing they had won the lottery and needed to pay taxes before collecting prize money, wired funds to the defendant. The defendant then transferred the fraudulently obtained funds to accounts outside the United States. As a result, the defendant took over $1 million from dozens of unsuspecting individuals. Further, the indictment alleged that the defendant knowingly made a false statement on an application for the renewal of a loan or line of credit with a financial institution. The defendant misrepresented their income from the scheme, disguising it as derived from the sale of bitcoin, and failed to disclose that it was fraudulently obtained.

The case was investigated by our office, the FBI, and the U.S. Department of Homeland Security's Homeland Security Investigations. It is being prosecuted by the U.S. Attorney's Office for the Western District of Texas.

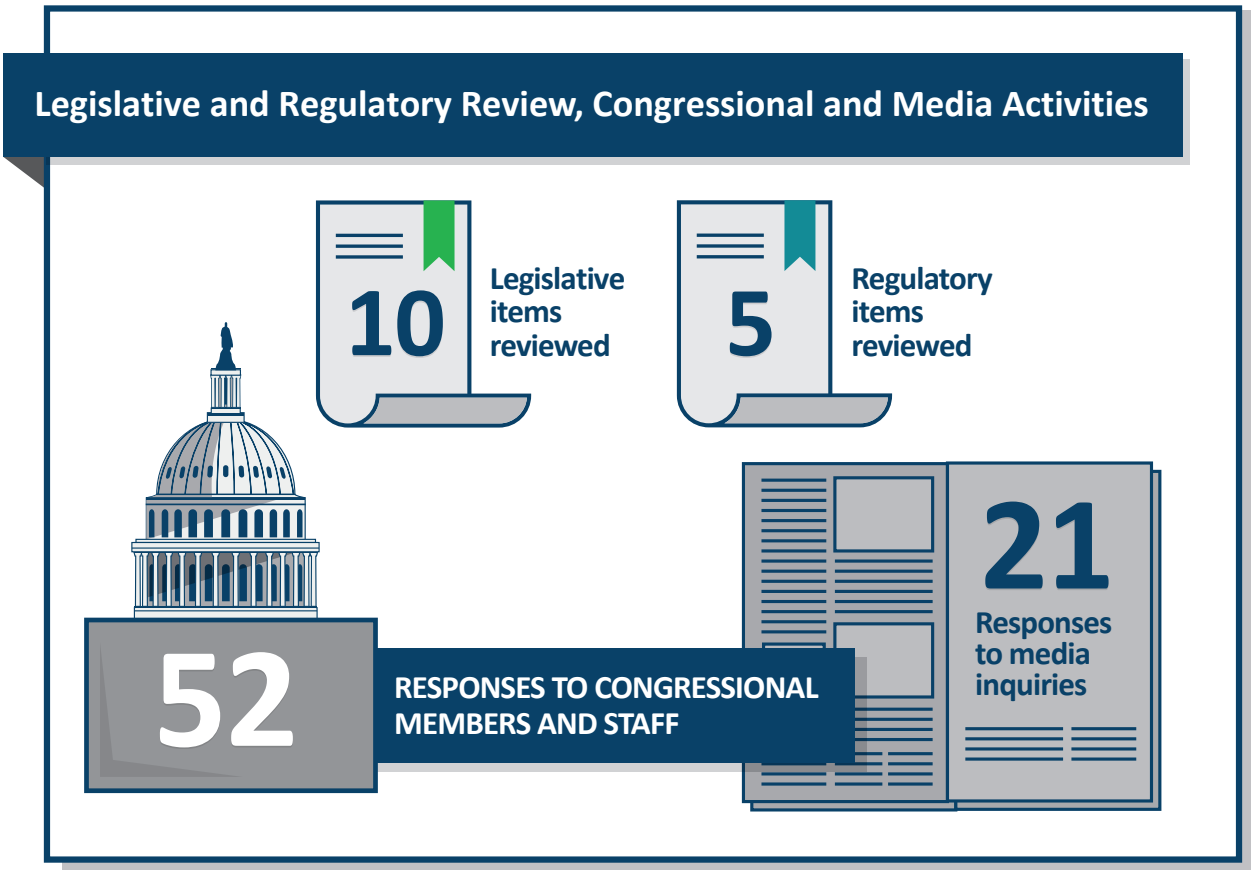
Hotline

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 642 complaints. Complaints within our 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. We refer such complaints to the appropriate federal agency for evaluation and resolution.

We continue to receive many noncriminal consumer complaints regarding consumer financial products and services. For these matters, we typically refer complainants to the consumer group of the appropriate federal regulator for the institution involved, such as the Bureau's Office of Consumer Response, Federal Reserve Consumer Help, or other law enforcement agencies as appropriate. In addition, we receive misdirected complaints regarding COVID-19 pandemic–related programs and operations. In such cases, we refer either the individual or the original complaint to the appropriate agency for further evaluation.

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



Legislative and Regulatory Review

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

In accordance with section 4(a)(2) of the Inspector General Act of 1978, as amended, Legal Services independently reviews newly enacted and proposed legislation and regulations to determine their potential effect on the economy and efficiency of the Board's and the Bureau's programs and operations. During this reporting period, Legal Services reviewed 10 legislative items and 5 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 52 responses to congressional members and staff concerning the Board and the Bureau. Additionally, we responded to 21 media inquiries. Noteworthy during this period was our deputy inspector general's participation in a cybersecurity roundtable hosted by minority members of the House Financial Services Committee to discuss our IT security work.

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 19,400 reports, detailing for fiscal year 2020 alone over $33 billion in potential savings and over 5,200 recommendations to improve programs across the federal government.

The IG serves as a member of CIGIE's Legislation Committee and Technology Committee and is the vice chair of the Investigations Committee. The Legislation Committee is the central point of information for legislative initiatives and congressional activities that may affect the OIG community, such as proposed cybersecurity legislation that was reviewed during the reporting period. The Technology Committee facilitates effective IT audits, evaluations, and investigations and provides a forum for the expression of the OIG community's perspective on governmentwide IT operations. The Investigations Committee advises the OIG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines. The IG is also a member of CIGIE's Diversity, Equity, and Inclusion Work Group. The Diversity, Equity, and Inclusion Work Group works to affirm, advance, and augment CIGIE's commitment to address a diverse, equitable, and inclusive workforce and workplace environment throughout the OIG community.

In addition, the IG serves on CIGIE's PRAC, which coordinates oversight of federal funds authorized by the CARES Act and the COVID-19 pandemic response. The IG is the vice chair of the PRAC Investigations

Subcommittee and is a member of the PRAC Financial Institutions Oversight Subcommittee. During this period, the IG, along with the FDIC IG, hosted a listening session with lenders and financial institutions concerning their experiences with the operation and administration of CARES Act programs and other pandemic response efforts of the federal government.

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 Legal Services attorneys are members of the Council of Counsels to the Inspector General, and our quality assurance staff founded and are current members of the Federal Audit Executive Council's Quality Assurance Work Group.

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 October 2020, the OIG for the National Archives and Records Administration completed a peer review of our audit organization. We received a peer review rating of *pass*.
- In August 2019, the OIG for the Tennessee Valley Authority completed the latest peer review of our Office of Investigations and rated us as compliant. There were no report recommendations, and we had no pending recommendations from previous peer reviews of our investigations organization.
- In November 2019, a team comprising the OIGs for the Federal Housing Finance Agency, the Tennessee Valley Authority, and the U.S. Department of Labor completed a peer review of our evaluations policies and procedures as well as a subset of evaluations completed. No rating was assigned because the review was conducted as part of a pilot program. The review found that we sufficiently met CIGIE's *Quality Standards for Inspection and Evaluation*. There were no report recommendations, but the review team did identify suggestions to improve our compliance with internal policies and procedures.

See our website for peer review reports of our organization.

Appendix A: Statistical Tables

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

Report title	Type of report
2020 Audit of the Board's Information Security Program	Audit
Calendar Year 2019 Risk Assessment of the Board's Government Travel Card Program	Risk assessment
Calendar Year 2019 Risk Assessment of the Board's Purchase Card Program	Risk assessment
The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis	Evaluation
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2020 and 2019, and Independent Auditors' Report	Audit
The Board Can Improve the Management of Its Renovation Projects	Audit
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2020 and 2019, and Independent Auditors' Report	Audit
Total number of audit reports: 4 Total number of evaluation reports: 1 Total number of other reviews: 2	

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
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	0	03/20	0	1
2016 Audit of the Board's Information Security Program	11/16	9	9	0	11/20	8	1
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing	04/17	8	8	0	03/21	7	1
2017 Audit of the Board's Information Security Program	10/17	9	9	0	11/20	5	4
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	03/21	13	1
Security Control Review of the Board's Public Website (nonpublic)	03/18	7	7	0	06/20	4	3
Security Control Review of the Board Division of Research and Statistics' General Support System (nonpublic)	09/18	9	9	0	03/20	7	2

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2018 Audit of the Board's Information Security Program	10/18	6	6	0	11/20	5	1
The Board Can Strengthen Information Technology Governance	11/18	6	6	0	06/20	3	3
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	11/20	8	0
The Board Can Enhance Its Internal Enforcement Action Issuance and Termination Processes by Clarifying the Processes, Addressing Inefficiencies, and Improving Transparency	09/19	6	6	0	03/21	4	2
The Board's Law Enforcement Operations Bureau Can Improve Internal Processes	09/19	6	6	0	03/21	4	2
2019 Audit of the Board's Information Security Program	10/19	6	6	0	11/20	1	5
The Board Should Finalize Guidance to Clearly Define Those Considered Senior Examiners and Subject to the Associated Postemployment Restriction	03/20	1	1	0	01/21	0	1

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board's Oversight of Its Designated Financial Market Utility Supervision Program Is Generally Effective, but Certain Program Aspects Can Be Improved	03/20	6	6	0	02/21	0	6
The Board Can Enhance Certain Aspects of Its Enforcement Action Monitoring Practices	03/20	1	1	0	03/21	0	1
The Board Can Further Enhance the Design and Implementation of Its Operating Budget Process	03/20	2	2	0	03/21	0	2
The Board Can Strengthen Its Oversight of the Protective Services Unit and Improve Controls for Certain Protective Services Unit Processes	03/20	6	6	0	03/21	5	1
The Board Can Improve Its Contract Administration Processes	03/20	13	13	0	03/21	11	2
The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced	09/20	10	10	0	03/21	4	6
2020 Audit of the Board's Information Security Program	11/20	4	4	0	n.a.	0	4
The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis	02/21	6	6	0	n.a.	0	6

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
The Board Can Improve the Management of Its Renovation Projects	03/21	2	2	0	n.a.	0	2

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

n.a. not applicable.

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

Report title	Type of report
2020 Audit of the Bureau's Information Security Program	Audit
Forensic Evaluation of the Bureau's Vendor Payment Process	Evaluation
The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce	Audit
Total number of audit reports: 2 Total number of evaluation reports: 1	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Management agrees	Management disagrees	Last follow-up date	Closed	Open
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	11/20	2	1
2016 Audit of the CFPB's Information Security Program	11/16	3	3	0	11/20	3	0
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	11/20	5	2
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	09/20	9	2
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	01/20	1	1
2018 Audit of the Bureau's Information Security Program	10/18	4	4	0	11/20	1	3
Technical Testing Results for the Bureau's SQL Server Environment (nonpublic)	05/19	5	5	0	03/21	0	5
The Bureau Can Improve The Effectiveness of Its Life Cycle Processes for FedRAMP	07/19	3	3	0	03/21	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
2019 Audit of the Bureau's Information Security Program	10/19	7	7	0	11/20	3	4
The Bureau's Office of Enforcement Has Centralized and Improved Its Final Order Follow-Up Activities, but Additional Resources and Guidance Are Needed	03/20	3	3	0	03/21	3	0
Testing Results for the Bureau's Plan of Action and Milestones Process	04/20	2	2	0	03/21	0	2
The Bureau Can Improve Its Periodic Monitoring Program to Better Target Risk and Enhance Training for Examiners	06/20	4	4	0	03/21	4	0
Technical Testing Results for the Bureau's Legal Enclave (nonpublic)	07/20	4	4	0	03/21	0	4
Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program	08/20	3	3	0	08/20	0	3
2020 Audit of the Bureau's Information Security Program	11/20	1	1	0	n.a.	0	1
The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce	03/21	10	10	0	n.a.	0	10

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	107
Investigations opened during the reporting period	31
Investigations closed during the reporting period	13
Investigations open at end of the reporting period	125
Investigative results for the reporting period	
Persons referred to DOJ prosecutors	21
Persons referred to state/local prosecutors	0
Declinations received	12
Joint investigations	102
Reports of investigation issued	0
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	19
Suspensions	0
Debarments	0
Prohibitions from banking industry	0
Indictments	19
Criminal informations	8
Criminal complaints	4
Convictions	9
Civil actions	$0

See notes at end of table.

Investigative actions	Number or dollar value[a]
Administrative monetary recoveries and reimbursements	$0
Civil judgments	$0
Criminal fines, restitution, and special assessments	$5,007,466
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	21
Complaints received during reporting period	642
Total complaints for reporting period	663
Complaints resolved during reporting period	633
Complaints pending	30

Appendix B: Inspector General Empowerment Act of 2016 Requirements

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

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

- We have no such instances to report.

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

- See appendix C.

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

- See table A-6.

A report on each investigation conducted by the OIG that involves a senior government employee in which allegations of misconduct were substantiated, which includes (1) the name of the senior government official, if already made public by the OIG; (2) a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter; (3) whether the

matter was referred to the DOJ and the date of the referral; and (4) whether the DOJ declined the referral and the date of such declination.

- We have no such instances to report.

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

- We have no such instances to report.

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

- We have no such attempts to report.

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

- We initiated an investigation concerning allegations that a senior Bureau employee was misusing official government time and allegations of other fraud, waste, and abuse. These allegations were unsubstantiated, and the investigation was closed.
- We initiated an investigation concerning allegations that a senior Bureau employee failed to take appropriate action regarding alleged timesheet and policy violations. These allegations were unsubstantiated, and the investigation was closed.

Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations

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

Board of Governors of the Federal Reserve System

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

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2013	1	1
2014	0	0
2015	0	0
2016	1	1
2017	3	6
2018	4	9
2019	3	9
2020	8	23
2021 [a]	2	8

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

a. Through March 31, 2021.

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.

2016 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 1

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

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

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: 1

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: 4

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: 1

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

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

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

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

Total number of recommendations: 7
Recommendations open: 3

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)

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

Total number of recommendations: 9
Recommendations open: 2

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

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

2018 Audit of the Board's Information Security Program

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

Total number of recommendations: 6
Recommendations open: 1

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

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

The Board Can Strengthen Information Technology Governance

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

Total number of recommendations: 6
Recommendations open: 3

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 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: 2

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

We found that the Board and the Reserve Banks have implemented some effective practices to support the enforcement action issuance and termination processes; however, we identified opportunities for the Board to enhance these processes. Specifically, we found that the Board can clarify certain aspects of these internal processes, such as the steps in these processes, the Board stakeholders' roles and responsibilities, and the Board members' involvement. In addition, we found that the Board can (1) improve the timeliness and efficiency of its enforcement action issuance and termination processes and (2) increase transparency with respect to the status of ongoing enforcement actions.

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

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

Total number of recommendations: 6
Recommendations open: 2

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

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

2019 Audit of the Board's Information Security Program

2019-IT-B-016 October 31, 2019

Total number of recommendations: 6
Recommendations open: 5

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

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

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

2020-SR-B-003 March 9, 2020

Total number of recommendations: 1
Recommendations open: 1

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

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

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

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

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

Total number of recommendations: 6
Recommendations open: 6

We assessed the effectiveness of the Board's oversight of its designated financial market utility (DFMU) supervision program.

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

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

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

Total number of recommendations: 1
Recommendations open: 1

We assessed the effectiveness of the Board's and the Reserve Banks' enforcement action monitoring practices, with a focus on supervised financial institutions within the community banking organization and the large and foreign banking organization portfolios.

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

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

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

Total number of recommendations: 2
Recommendations open: 2

We assessed the design and implementation of the Board's processes for formulating and executing its annual operating budget.

The Board has made changes over the past several years to improve its budget process; the Board has acknowledged perennial underspending and is addressing it by focusing on slowing growth and spending more consistently with budget estimates. The Board can further enhance the design and implementation of its operating budget process by communicating its budget process in an overarching document, strengthening the connection between budget and strategy, and implementing an agencywide approach to executing the approved budget.

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

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

Total number of recommendations: 6
Recommendations open: 1

We assessed the Internal Oversight Committee's 2018 evaluation of the Protective Services Unit (PSU), as well as the PSU's operations to support its mission.

The 2018 Internal Oversight Committee evaluation of PSU operations generally complied with the committee's guidance, although we found opportunities for improvement that could strengthen future evaluations of the PSU's operations. In our assessment of PSU operations, we found that the PSU complied

with its policies and procedures for certain aspects of protection measures and protective intelligence. However, the PSU (1) does not have procedures related to vehicle maintenance, (2) does not require driving refresher training for special agents, and (3) did not consistently maintain records of destroyed credentials for separated agents.

The Board Can Improve Its Contract Administration Processes

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

Total number of recommendations: 13
Recommendations open: 2

We assessed the Board's compliance with laws, regulations, and Board policies and procedures applicable to contract administration, as well as the effectiveness of the Board's internal controls related to contract administration. We focused on the Board's contract administration processes from postaward to contract closeout.

We found that the Division of Financial Management can improve its contract administration processes as well as related internal controls. In addition, contracting officer's representatives do not appear to be adequately trained to fulfill their responsibilities.

The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced

2020-SR-B-019 **September 30, 2020**

Total number of recommendations: 10
Recommendations open: 6

We assessed the effectiveness of the Board's cybersecurity supervision approach for Large Institution Supervision Coordinating Committee (LISCC) firms—the largest, most systemically important domestic and foreign financial institutions supervised by the Board.

The Board's approach to cybersecurity supervision of LISCC firms continues to evolve and can be enhanced. The Board can strengthen its governance of LISCC firm cybersecurity supervision by clarifying the roles and responsibilities of the groups involved in supervision and planning activities and better defining how cybersecurity supervisory activities inform relevant ratings. The Board can also enhance its approach to cybersecurity training to ensure examiners keep their skills up to date. Additionally, the Board can improve its guidance and training for reporting cybersecurity events.

2020 Audit of the Board's Information Security Program

2020-IT-B-020 **November 2, 2020**

Total number of recommendations: 4
Recommendations open: 4

See the summary in the body of this report.

The Board Economics Divisions Can Enhance Some of Their Planning Processes for Economic Analysis

2021-MO-B-001 **February 24, 2021**

Total number of recommendations: 6
Recommendations open: 6

See the summary in the body of this report.

The Board Can Improve the Management of Its Renovation Projects

2021-FMIC-B-004 **March 10, 2021**

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

Bureau of Consumer Financial Protection

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

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2014	1	1
2015	0	0
2016	0	0
2017	1	2
2018	3	6
2019	3	12
2020	4	10
2021[a]	1	10

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

a. Through March 31, 2021.

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.

2017 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 7
Recommendations open: 2

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

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

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

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

Total number of recommendations: 11
Recommendations open: 2

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

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

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

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

Total number of recommendations: 2
Recommendations open: 1

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

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

2018 Audit of the Bureau's Information Security Program

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

Total number of recommendations: 4
Recommendations open: 3

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

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

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

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

Total number of recommendations: 5
Recommendations open: 5

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

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

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

Total number of recommendations: 3
Recommendations open: 3

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

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

2019 Audit of the Bureau's Information Security Program

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

Total number of recommendations: 7
Recommendations open: 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 effectively at a level-4 (*managed and measurable*) maturity. We identified opportunities for the Bureau to strengthen its information security program in FISMA domains across all five Cybersecurity Framework security functions—*identify*, *protect*, *detect*, *respond*, and *recover*—to ensure that its program remains effective.

Testing Results for the Bureau's Plan of Action and Milestones Process

2020-IT-C-014 **April 29, 2020**

Total number of recommendations: 2
Recommendations open: 2

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested the Bureau's plan of action and milestones (POA&M) process, which the agency uses to document and remediate information security weaknesses.

We found that costs associated with remediating cybersecurity weaknesses listed in POA&Ms were not accurately accounted for. We also identified instances in which the status of cybersecurity weaknesses included in the Bureau's automated solution for POA&M management was inaccurate.

Technical Testing Results for the Bureau's Legal Enclave (nonpublic)

2020-IT-C-017R **July 22, 2020**

Total number of recommendations: 4
Recommendations open: 4

As part of our 2019 audit of the Bureau's information security program, which we performed to meet FISMA requirements, we tested technical controls for the agency's Legal Enclave.

We found a significant weakness on a device that controls access to the environment housing the Legal Enclave, resulting in several security vulnerabilities. Further, the Bureau had not appropriately tested contingency planning activities for the device. In addition, we identified several security misconfigurations and security weaknesses for technologies in the Legal Enclave, which increase the risk of unauthorized data access and system misuse. Although the Bureau was aware of several of these issues, it had not taken timely action to mitigate the risks; the Bureau had accepted specific risks related to certain vulnerabilities in the Legal Enclave but had not formally documented its rationale for these decisions.

Results of Scoping and Suspension of the Evaluation of the Bureau's Personnel Security Program

2020-MO-C-018 **August 17, 2020**

Total number of recommendations: 3
Recommendations open: 3

We initiated an evaluation to assess the efficiency and effectiveness of the Bureau's personnel security program. However, the Bureau recently completed an internal review of the program, which identified other areas for improvement, and the U.S. Office of Personnel Management launched a separate review in March 2020. Because the Bureau needs time to fully address the results from these additional reviews, we suspended our evaluation.

We found that the Personnel Security Office does not have measurable objectives to evaluate its performance related to reducing its adjudication backlog, nor does it have a plan with measurable objectives to manage the background investigation process going forward. In addition, we found that the Personnel Security Office does not have processes to reconcile its personnel security data.

2020 Audit of the Bureau's Information Security Program

2020-IT-C-021 **November 2, 2020**

Total number of recommendations: 1
Recommendations open: 1

See the summary in the body of this report.

The Bureau Can Strengthen Its Hiring Practices and Can Continue Its Efforts to Cultivate a Diverse Workforce

2021-MO-C-006 **March 30, 2021**

Total number of recommendations: 10
Recommendations open: 10

See the summary in the body of this report.

Abbreviations

CARES Act	Coronavirus Aid, Relief, and Economic Security Act
CEO	chief executive officer
CFPB	Consumer Financial Protection Bureau
CI	Criminal Investigation
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
DATA Act	Digital Accountability and Transparency Act of 2014
DFMU	designated financial market utility
DOJ	U.S. Department of Justice
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
IG	inspector general
IRS	Internal Revenue Service
IT	information technology
LEU	Law Enforcement Unit
LISCC	Large Institution Supervision Coordinating Committee
MDPS	multiregional data processing servicer
PIIA	Payment Integrity Information Act of 2019
POA&M	plan of action and milestones
PPP	Paycheck Protection Program
PRAC	Pandemic Response Accountability Committee
PSU	Protective Services Unit
SBA	U.S. Small Business Administration
SBLC	Standby Letter of Credit

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