Office of Inspector General

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

Semiannual Report to Congress

October 1, 2017–March 31, 2018

OIG

Semiannual Report to Congress

October 1, 2017–March 31, 2018

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

Message From the Inspector General

Since our last semiannual report to Congress in October 2017, both agencies that we oversee have come under new leadership. After serving as a Governor since 2012, Jerome Powell took office as the Chairman of the Board of Governors of the Federal Reserve System (Board) in February 2018. Mick Mulvaney became the Acting Director of the Consumer Financial Protection Bureau (CFPB) in November 2017. We've met several times with Chairman Powell and Acting Director Mulvaney to brief them on our past, ongoing, and planned work and to discuss their priorities and any concerns they may have with their programs and operations. We look forward to continuing to work with both leaders to provide independent oversight of their respective agencies in order to improve their programs and operations and to prevent and detect fraud, waste, and abuse.

During the past 6 months, we issued seven reports related to the Board's programs. These reports cover a broad range of topics, including the Board's governance structure, information technology, building infrastructure, procurement, and human capital. We issued five reports on the CFPB's operations—four focused on information technology and related security efforts, and one on the CFPB's process for offboarding employees and contractors.

Also of note, we released our first OIG Insights paper. OIG Insights papers are designed to describe lessons learned from our audit and evaluation work that have applicability beyond the program reviewed and the agencies we oversee. In this paper, we address the root causes for employees' reticence to share their views with leaders. We also describe steps leaders can take to address these causes and to monitor progress.

In addition, we provided the agencies' new leadership with independent investigative oversight. Our Office of Investigations pursued bank fraud, particularly by senior bank executives, and other cases involving the supervision programs of both agencies, as well as cases related to the agencies' internal operations. Specifically, we handled 412 new hotline complaints and closed 15 investigations. Our work resulted in 3 persons referred for criminal prosecution; an indictment; a conviction of a former bank executive and a guilty plea from another; and over $46 million in civil actions, criminal fines, restitution, special assessments, and forfeitures. Through our investigative work, we continue to send a clear message that those who commit wrongdoing against the Board or the CFPB will be brought to justice. We also demonstrated our ongoing commitment to strengthening relationships with our law enforcement partners by hosting conferences that drew attendees from dozens of federal, state, and local law enforcement agencies.

The work of an Office of Inspector General demands that we be independent, fact based, and trustworthy. Every day, I am inspired by my staff's devotion to these principles and grateful for the high-quality work they produce.

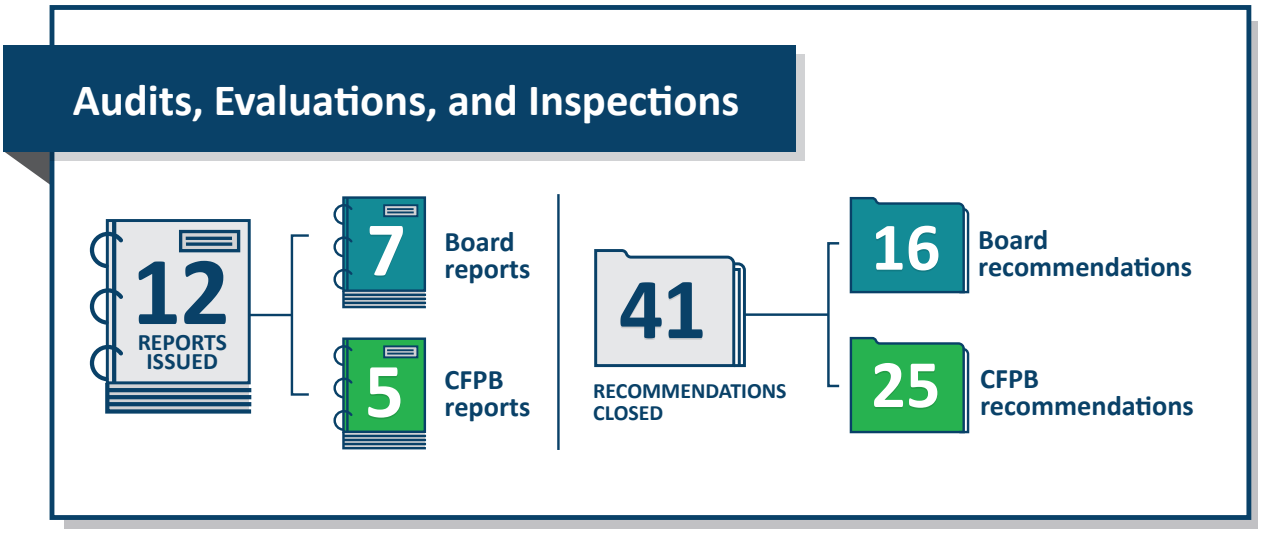
Sincerely,

Mark Bialek
Inspector General
April 30, 2018

Contents

Highlights

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



The Board's Information Security Program

The Board has taken several steps to mature its information security program to ensure that it is consistent with Federal Information Security Modernization Act of 2014 (FISMA) requirements. However, the Board's information security program needs several improvements in the areas of risk management, information technology services centralization, configuration management, and information security continuous monitoring.

Leadership and Management Best Practices on Encouraging Divergent Views

We issued our first OIG Insights paper, based on an evaluation we conducted regarding employees' willingness to share their views about large financial institution supervision activities. We identified widely applicable best practices that leaders can follow to increase employees' willingness to share their views. These best practices include soliciting viewpoints regularly, modeling a willingness to challenge up the chain of command, recognizing employees who speak up, explaining the rationale for decisions, and acknowledging their own mistakes.

The Board's Organizational Governance System

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 to enable it to more effectively and efficiently achieve its objectives.

The Failure of Allied Bank

The Board can improve supervisory processes by clarifying when Federal Reserve Banks should report suspicious activity detected during bank examination activities to law enforcement officials and enhance communication between the Board's Legal Division and the Reserve Banks following requests for an enforcement action.

The CFPB's Information Security Program

The CFPB has taken several steps to mature its information security program to ensure that it is consistent with FISMA requirements. However, the CFPB's information security program needs several improvements in the areas of enterprise risk management, configuration monitoring, multifactor authentication, security awareness and training, and incident response and contingency planning.

The CFPB's Offboarding Processes and Data

The CFPB has offboarding controls related to conflicts of interest for executive employees' postemployment restrictions; however, the CFPB has opportunities to strengthen controls related to other components of the employee offboarding process.

Former President and Chief Executive Officer of Farmers Exchange Bank Sentenced

The former President and Chief Executive Officer of Farmers Exchange Bank in Wisconsin was sentenced to 24 months' imprisonment for bank fraud; false entries, reports, and transactions; and false statements. The defendant was also fined $20,000 and ordered to pay $338,000 in restitution to the bank holding company shareholders. Finally, the defendant was prohibited from further participation in the banking industry by the Board and the Federal Deposit Insurance Corporation (FDIC).

Former Chief Executive Officer and President Pleaded Guilty to Conspiracy to Commit Bank Fraud and Obstruction of Examination

A former Chief Executive Officer and President at Coastal Bank and Trust, based in North Carolina, pleaded guilty to conspiracy to commit bank fraud and obstruction of examination. The defendant schemed to defraud the bank by engineering fraudulent loan transactions to straw borrowers for his own benefit or for that of his coconspirators. The defendant attempted to conceal his scheme by withholding relevant information from the bank's board of directors and from Federal Reserve Bank examiners.

Wilmington Trust Corporation Entered Into Settlement Agreement

In a settlement, Delaware's Wilmington Trust Corporation agreed to transfer $44 million to the United States. Wilmington Trust agreed to the settlement in lieu of prosecution for criminal false statements and false entries in banking records related to its past-due loans.

Introduction

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

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

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

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

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

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

1. CIGFO comprises the IGs of the Board and the CFPB, the Commodity Futures Trading Commission, the U.S. Department of Housing and Urban Development, the U.S. Department of the Treasury, the FDIC, the Federal Housing Finance Agency, the National Credit Union Administration, the U.S. Securities and Exchange Commission, and the Office of the Special Inspector General for the Troubled Asset Relief Program.
2. The FFIEC is a formal interagency body empowered (1) to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board, the FDIC, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the CFPB and (2) to make recommendations to promote uniformity in the supervision of financial institutions.

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

Audits, Evaluations, and Inspections

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

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

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

Board of Governors of the Federal Reserve System

2017 Audit of the Board's Information Security Program

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

To meet our annual FISMA reporting responsibilities, 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 did so according to U.S. Department of Homeland Security guidelines, which involves evaluating the program's maturity level (from a low of 1 to a high of 5) across several areas.

The Board's information security program is operating at a level-3 maturity (*consistently implemented*), with the agency performing several activities indicative of a higher maturity level. Further, it has implemented an effective security training program that includes phishing exercises and associated performance metrics.

However, the Board can mature its information security program to ensure that it is effective, or operating at level-4 maturity (*managed and measurable*). The lack of an agencywide risk-management governance structure and strategy as well as decentralized information technology services result in an incomplete view of the risks affecting the security posture of the Board and impede its ability to implement an effective information security program. In addition, several security processes, such as configuration management and information security continuous monitoring, were not effectively implemented agencywide.

As of October 31, 2017, the Board had taken sufficient action to close 6 of 10 recommendations from our prior FISMA audits. In this report, we added recommendations designed to strengthen the Board's information security program in the areas of risk management, configuration management, identity and access management, information security continuous monitoring, and contingency planning. The Board concurred with our recommendations.

Leadership and Management Best Practices to Increase Employee Willingness to Share Views

November 15, 2017

Summarizing insights from our 2016 evaluation that assessed employees' willingness to share their views about large financial institution supervision activities that may have broader applicability for other leaders and managers, this paper describes the root causes that contribute to employees' reticence to speak up, such as the perception that management will not act on their views or the fear of retaliation during the performance management process.[3]

To address the root causes for employee reticence to share, leaders can follow best practices, such as soliciting viewpoints regularly, modeling a willingness to challenge up the chain of command, recognizing employees who speak up, explaining the rationale for decisions, and acknowledging their own mistakes. Monitoring progress on these efforts can help ensure that they are effective.

Increasing employees' willingness to share their views can improve the flow of information to leaders and support informed decisionmaking.

3. Office of Inspector General, *Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities*, OIG Report 2016-SR-B-014, November 14, 2016.

The Board's Organizational Governance System Can Be Strengthened

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

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
- establishing and documenting the Executive Committee's mission, protocols, and authorities

Strengthening its core governance structures should enable the Board to more efficiently and effectively achieve its objectives.

Our report contains recommendations designed to strengthen the Board's organizational governance structures. The Board generally concurred with our recommendations.

Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2017 and 2016, and Independent Auditors' Reports

2018-FMIC-B-004 **February 27, 2018**

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

Auditing Standards issued by the U.S. Comptroller General. We reviewed and monitored the work of the independent public accounting firm to ensure compliance with applicable standards and the contract.

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the FFIEC as of December 31, 2017 and 2016, and the results of operations and cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America. The auditors' report on internal control over financial reporting and on compliance and other matters disclosed no instances of noncompliance or other matters.

Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2017 and 2016, and Independent Auditors' Reports

2018-FMIC-B-005 March 5, 2018

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

In the auditors' opinion, the financial statements presented fairly, in all material respects, the financial position of the Board as of December 31, 2017 and 2016, and the results of its operations and its cash flows for the years then ended in conformity with accounting principles generally accepted in the United States of America. Also, in the auditors' opinion, the Board maintained, in all material respects, effective internal control over financial reporting as of December 31, 2017, 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.

Security Control Review of the RADAR Data Warehouse

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

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

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

Our report includes recommendations to strengthen the security of the RADAR Data Warehouse as well as three matters for management's consideration. The Board concurred with our recommendations.

Review of the Failure of Allied Bank

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

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

Allied Bank failed because of corporate governance weaknesses and asset quality deterioration resulting from deficient credit risk-management practices. Ineffective oversight by Allied Bank's board of directors allowed two management officials to exert a dominant influence over the bank's affairs, including lending decisions, and allegedly engage in insider abuse. Allied Bank's management also failed to establish adequate credit risk-management practices commensurate with the risks in the bank's loan portfolio. Weak credit underwriting and administration practices resulted in violations of certain regulations and bank lending policies, significant loan concentrations, and an excessive volume of classified assets. The bank's asset quality deterioration significantly impaired profitability and eventually depleted the bank's capital levels, resulting in the bank's failure.

Although the Federal Reserve Bank of St. Louis took decisive supervisory action to address Allied Bank's weaknesses, it could have also recommended that the Board report suspicious activity to law enforcement when the Reserve Bank first identified signs of insider abuse. Our review resulted in a finding related to Suspicious Activity Report filings by the Federal Reserve System and a finding related to enhanced communication between the Board's Legal Division and the Reserve Banks.

Our report contains recommendations designed to improve supervisory processes and to enhance communication between the Board's Legal Division and the Reserve Banks following requests for enforcement action. The Board concurred with our recommendations.

Security Control Review of the Board's Public Website

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

The Board's public website provides a large and diverse audience with timely and accurate information about the mission and work of the Board. To meet FISMA requirements, 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 improvement opportunities in the areas of configuration management and risk management.

Our report includes recommendations to strengthen the security of the Board's public website in these areas. The Board concurred with our recommendations.

Consumer Financial Protection Bureau

The CFPB Met DATA Act Submission Requirements

2017-FMIC-C-017 **October 23, 2017**

The DATA Act aims to help policymakers and the public follow the flow of federal dollars by requiring agencies to submit certain spending data to USAspending.gov. We audited the CFPB's compliance with the DATA Act. Specifically, we assessed (1) the completeness, timeliness, accuracy, and quality of the CFPB's fiscal year 2017 second quarter financial and award data submitted for publication on USAspending.gov and (2) the CFPB's implementation and use of the governmentwide financial data standards established by OMB and Treasury, as applicable.

The CFPB met DATA Act submission requirements. All data in our sample were complete, timely, accurate, and of good quality. In addition, the CFPB followed the applicable governmentwide financial data standards established by OMB and Treasury. Our report contains no recommendations.

2017 Audit of the CFPB's Information Security Program

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

To meet our annual FISMA reporting responsibilities, we evaluated the effectiveness of the CFPB's (1) security controls and techniques for select information systems and (2) information security policies, procedures, and practices. We did so according to U.S. Department of Homeland Security guidelines, which involves evaluating the program's maturity level (from a low of 1 to a high of 5) across several areas.

The CFPB'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 CFPB 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 internal network and systems, assessments of the effectiveness of security awareness and training activities, and incident response and contingency planning capabilities.

As of October 31, 2017, the CFPB had taken sufficient action to close one of the four recommendations from our prior FISMA audits. In this report, we added recommendations designed to strengthen the CFPB's information security program. The CFPB concurred with our recommendations.

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

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

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

Our report contains recommendations designed to strengthen the CFPB's controls over the offboarding processes for the return of property, records management, and maintenance of contractor nondisclosure agreements. Additional recommendations include ensuring that the CFPB has an up-to-date list of its contractors as well as current, accurate, and complete separation data for contractors and employees. The CFPB concurred with our recommendations.

Audit of the CFPB's Encryption of Data on Mobile Devices

2018-IT-C-002R **January 25, 2018**

Mobile devices can help CFPB staff carry out their duties, but the portability of these devices heightens the risk of loss or theft of information technology equipment and data. We therefore evaluated (1) the effectiveness of the CFPB's techniques for encrypting data on mobile devices and (2) the strength of the encryption methods and the password complexity and reset rules applied.

The CFPB has an effective process for encrypting the data on its mobile devices, including full-disk encryption on its laptops and a native encryption solution on its smartphones. The encryption methods meet federal requirements, and the agency's password complexity and reset rules are adequate.

However, the CFPB has not been able to fully account for all laptops assigned to users since its establishment. In June 2016, we issued an early alert memorandum to the CFPB in which we identified a number of steps that the agency should take to gain assurance that unaccounted-for laptops do not present an unacceptable level of risk to the agency and to strengthen technical controls over protecting sensitive data. The CFPB took steps to assess the effect of the loss of the unaccounted-for laptops and strengthen controls for protecting sensitive data on mobile devices but did not complete all the steps outlined in our early alert memorandum related to the data access actions of individuals to whom the unaccounted-for laptops were assigned.

Integrating specific activities for managing the risk posed by sensitive data on unaccounted-for laptops, such as role-based analysis and system log reviews, will strengthen the CFPB's ongoing efforts to develop and implement an insider threat program and incident containment strategies. The CFPB concurred with our suggestion.

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

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

We contracted with Cotton & Company to conduct a performance audit of the CFPB's privacy program and its implementation. The contract requires the audit to be performed in accordance with generally

accepted government auditing standards. We reviewed and monitored the work of Cotton & Company to ensure compliance with the contract.

Overall, Cotton & Company found that the CFPB 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 CFPB has documented privacy policies and procedures covering a wide range of topics, including privacy roles and responsibilities, privacy impact assessment and system of records notice management, training, breach notification and response, and monitoring and auditing.

The Cotton & Company report includes recommendations designed to strengthen the CFPB's privacy and security program. The CFPB concurred with the recommendations.

Failed State Member Bank Reviews

Material Loss Reviews

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

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

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

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

Nonmaterial Loss Reviews

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

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

The IG must semiannually report the completion dates for each such review. If an in-depth review is not warranted, the IG is required to explain this determination. In general, we consider a loss to the DIF to present unusual circumstances if the conditions associated with the bank's deterioration, ultimate closure, and supervision were not addressed in any of our prior bank failure reports, or if there was potential fraud.

No state member bank failures occurred during the reporting period that required us to initiate a nonmaterial loss review. During the prior reporting period, we completed our initial review of the Fayette County Bank failure and identified a series of unusual circumstances that warrant an in-depth review. We will summarize the results of our in-depth review in an upcoming semiannual report to Congress.

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

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

Investigations

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

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

Board of Governors of the Federal Reserve System

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

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

Former President and Chief Executive Officer of Farmers Exchange Bank Sentenced

The former President and Chief Executive Officer of Farmers Exchange Bank in Neshkoro, Wisconsin, was sentenced in the U.S. District Court for the Eastern District of Wisconsin to concurrent terms of

24 months' imprisonment for each of the counts to which he pleaded guilty. The defendant pleaded guilty to three counts of bank fraud; one count of false entries, reports, and transactions; and one count of false statements. The defendant was also fined $20,000.00, ordered to pay a $500.00 special assessment, and ordered to pay restitution to the bank holding company shareholders in the amount of $338,000.00 pursuant to the terms of his plea agreement. Upon release from prison, the defendant will be on supervised release for a term of 24 months. The Board prohibited the defendant from further participation in the banking industry. We reported on the defendant's guilty plea in our April 1, 2017–September 30, 2017, semiannual report to Congress.

The defendant made false entries in the books, reports, and statements of the bank with intent to injure and defraud the bank, other bank officers, and other individuals and to deceive the agents and examiners appointed to examine the affairs of the bank, including the FDIC and the Board. The defendant also devised a scheme to defraud other FEB Bancshares, Inc., shareholders and to obtain money by means of false and fraudulent pretenses.

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

Former Chief Executive Officer and President Pleaded Guilty to Conspiracy to Commit Bank Fraud and Obstruction of Examination

A former Chief Executive Officer and President at Coastal Bank and Trust, based in Jacksonville, North Carolina, pleaded guilty in the U.S. District Court in the Eastern District of North Carolina to one count of conspiracy to commit bank fraud and one count of obstruction of examination. The plea was filed in May 2017, but the information was under seal until December 2017.

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

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

Wilmington Trust Corporation Entered Into Settlement Agreement in Lieu of Criminal Prosecution

On October 10, 2017, the U.S. Attorney's Office for the District of Delaware entered into a settlement agreement with Wilmington Trust Corporation, a state member bank supervised by the Board. As part of the agreement, Wilmington Trust agreed to transfer $44 million to the United States. The forfeiture by Wilmington Trust was agreed to by all parties in lieu of prosecution of the bank as specified in a superseding indictment, filed on January 6, 2016, for criminal violations including 18 U.S.C. §1001, False Statements, and 18 U.S.C. §1005, False Entries in Banking Records.

Per the settlement agreement, in connection with both its internal and external reporting of past-due loans, Wilmington Trust engaged in the waiver practice on a monthly basis whereby the bank excluded from final past-due numbers its matured commercial loans that were current for interest and in the process of extension. On 10 occasions from October 30, 2009, to July 23, 2010, the bank submitted a Monthly Regulatory Report to the Board that did not describe the bank's use of the waiver practice.

Additionally, in advance of a target examination of the bank by the Board that commenced in December 2009 and a full-scope examination that commenced in May 2010, the Board requested that the bank submit a list of its past-due loans. According to the settlement agreement, in responding to each request, the bank's submissions did not describe its use of the waiver practice.

The bank's waiver practice resulted in a variance between commercial loans treated as past due within its internal records and reported publicly as past due on its Consolidated Reports of Condition and Income and in its Monthly Regulatory Reports.

This investigation was conducted by our office, the FBI, the Internal Revenue Service–Criminal Investigation, and the Office of the Special Inspector General for the Troubled Asset Relief Program and prosecuted by the U.S. Attorney's Office for the District of Delaware.

Consumer Financial Protection Bureau

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

The CFPB supervises large banks, thrifts, and credit unions with total assets of more than $10 billion and certain nonbank entities, regardless of size, including mortgage brokers, loan modification providers, payday lenders, consumer reporting agencies, debt collectors, and private education lenders. Additionally, with certain exceptions, the CFPB'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 CFPB's responsibilities typically involve allegations that company directors or officers provided falsified business data and financial records to the CFPB, lied to or misled examiners, or obstructed examinations in a manner that may have affected the CFPB's ability to carry out its supervisory responsibilities. Such activity may result in criminal violations, such as false statements or obstruction of examinations. The following is an example from this reporting period of an investigation into matters affecting the CFPB's ability to carry out its supervisory responsibilities.

Remaining Principals of Loan Modification Company Sentenced

Multiple principals of a loan modification company were sentenced in the U.S. District Court for the District of Utah for their involvement in a fraudulent telemarketing sales and loan modification conspiracy. The individuals previously had pleaded guilty to conspiracy to commit mail fraud and money laundering in an alleged scheme to market and sell home loan modification services under the guise of a law firm. During sentencing, a co-owner of the loan modification company was sentenced to 12 months and 1 day's imprisonment and 36 months' supervised release. He was also ordered to forfeit $886,915.72 from seized assets and was ordered to pay $415,940.01 in restitution and a $100.00 special assessment. A second individual, a Sales Manager, was sentenced to 60 months' probation, ordered to forfeit $259,528.12 by money judgment order, and ordered to pay $121,711.82 restitution and a $100.00 special assessment. A third individual, also a Sales Manager, was sentenced to 60 months' probation, ordered to forfeit $232,400.69 by money judgment order, and ordered to pay $108,989.78 restitution and a $100.00 special assessment. We reported on the sentencing of the other co-owner and another Sales Manager in our April 1, 2017–September 30, 2017, semiannual report to Congress.

Around September 2011, the principals and others made false and misleading statements to potential customers in order to convince them to pay for loan modification services. Potential clients were led to believe they were contracting with a true law firm, that an attorney would be working with them individually, and that the attorney would negotiate a loan modification with their lender. Instead, clients were contacted by the defendant and minimum-wage employees who were not supervised by lawyers and did not have a legal background or knowledge about working loan modifications.

This case was investigated by our office, the FBI, Internal Revenue Service–Criminal Investigation, the Office of the Special Inspector General for the Troubled Asset Relief Program, and the Federal Housing Finance Agency OIG and prosecuted by the U.S. Attorney's Office for the District of Utah.

Hotline

The OIG Hotline helps people report fraud, waste, abuse, and mismanagement related to the programs or operations of the Board and the CFPB. 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 412 complaints. It continued to receive complaints from individuals seeking information about or wanting to file noncriminal consumer complaints regarding consumer financial products and services. In these matters, OIG Hotline staff members typically refer complainants to the consumer group of the appropriate federal regulator for the institution involved, such as the Office of the Comptroller of the Currency's (OCC) Customer Assistance Group or the CFPB Consumer Response team.

The OIG Hotline also continued to receive a significant number of complaints involving suspicious solicitations invoking the name of the Federal Reserve or the Chair of the Board of Governors. Hotline staff members continue to advise all individuals that these phishing emails are solicitations that attempt to obtain the personal or financial information of the recipient and that neither the Board nor the Reserve Banks endorse or have any involvement in them. As appropriate, we investigate these complaints.

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

Legislative and Regulatory Review

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

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 CFPB's programs and operations. During this reporting period, Legal Services reviewed 10 legislative items and 11 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 41 responses to congressional members and staff concerning the Board and the CFPB. Additionally, we responded to 14 media inquiries.

CIGIE Participation

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

As part of the IG community, we are proud to be part of the Oversight.gov effort. Oversight.gov is a new, searchable website containing the latest public reports from federal IGs. It provides access to more than 8,000 reports, detailing for fiscal year 2017 alone over $23 billion in potential savings and over 9,000 recommendations to improve programs across the federal government.

The IG serves as a member of CIGIE's Legislation Committee and Investigations Committee. The Legislation Committee is the central point of information for legislative initiatives and congressional activities that may affect the IG community, such as proposed cybersecurity legislation that was reviewed during the reporting period. The Investigations Committee advises the IG community on issues involving criminal investigations, criminal investigations personnel, and criminal investigative guidelines.

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

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

Peer Reviews

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

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

See our website for peer review reports of our organization.

Appendix A: Statistical Tables

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

Report title	Type of report
2017 Audit of the Board's Information Security Program	Audit
The Board's Organizational Governance System Can Be Strengthened	Evaluation
Federal Financial Institutions Examination Council Financial Statements as of and for the Years Ended December 31, 2017 and 2016, and Independent Auditors' Reports	Audit
Board of Governors of the Federal Reserve System Financial Statements as of and for the Years Ended December 31, 2017 and 2016, and Independent Auditors' Reports	Audit
Security Control Review of the RADAR Data Warehouse	Audit
Review of the Failure of Allied Bank	Evaluation
Security Control Review of the Board's Public Website	Audit
Total number of audit reports: 5	
Total number of evaluation reports: 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	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Response to a Congressional Request Regarding the Economic Analysis Associated with Specified Rulemakings	06/11	2	2	0	03/18	0	2
Evaluation of Prompt Regulatory Action Implementation	09/11	1[a]	1	0	03/18	1	0
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	0	09/16	7	1
Security Control Review of the Board's Public Website (nonpublic report)	04/12	12	12	0	02/18	12	0
Board Should Enhance Compliance with Small Entity Compliance Guide Requirements Contained in the Small Business Regulatory Enforcement Fairness Act of 1996	07/13	2	2	0	03/18	2	0

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. 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	03/18	0	1
Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	07/14	3[a]	3	0	03/18	1	2
Opportunities Exist to Enhance the Board's Oversight of Future Complex Enforcement Actions	09/14	5	5	0	03/18	3	2
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board's Information Security Life Cycle	12/14	3	3	0	03/17	2	1
Review of the Failure of Waccamaw Bank	03/15	5	5	0	03/18	3	2
Security Control Review of the Board's Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)	09/15	3	3	0	n.a.	0	3

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
2015 Audit of the Board's Information Security Program	11/15	4	4	0	10/17	4	0
Security Control Review of the Board's Statistics and Reserves System (nonpublic report)	12/15	6	6	0	11/17	4	2
The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations	04/16	9	9	0	09/17	8	1
Security Control Review of the Board's Active Directory Implementation (nonpublic report)	05/16	10	10	0	02/18	1	9
2016 Audit of the Board's Information Security Program	11/16	9	9	0	10/17	5	4
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	0	03/18	2	9

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
The Board Can Improve Documentation of Office of Foreign Assets Control Examinations	03/17	2	2	0	n.a.	0	2
The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool	03/17	2	2	0	03/18	0	2
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing	04/17	8	8	0	n.a.	0	8
The Board Can Strengthen Its Guidance and Planning Efforts for Future Evaluations of the Law Enforcement Unit	08/17	3	3	0	n.a.	0	3
2017 Audit of the Board's Information Security Program	10/17	9	9	0	n.a.	0	9
The Board's Organizational Governance System Can Be Strengthened	12/17	14	14	0	n.a.	0	14
Security Control Review of the RADAR Data Warehouse (nonpublic report)	03/18	3	3	0	n.a.	0	3

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Review of the Failure of Allied Bank	03/18	2	2	0	n.a.	0	2
Security Control Review of the Board's Public Website (nonpublic report)	03/18	7	7	0	n.a.	0	7

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

n.a. not applicable.

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

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

Report title	Type of report
The CFPB Met DATA Act Submission Requirements	Audit
2017 Audit of the CFPB's Information Security Program	Audit
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	Audit
Audit of the CFPB's Encryption of Data on Mobile Devices	Audit
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	Audit
Total number of audit reports: 5 Total number of evaluation reports: 0	

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

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity	09/13	14	14	0	12/17	12	2
Security Control Review of the CFPB's Cloud Computing–Based General Support System (nonpublic report)	07/14	4	4	0	09/16	1	3
Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services	09/14	4	4	0	01/18	4	0
2014 Audit of the CFPB's Information Security Program	11/14	3	3	0	10/17	2	1
The CFPB Can Enhance Its Diversity and Inclusion Efforts	03/15	17	17	0	03/18	16	1
The CFPB Can Enhance Its Contract Management Processes and Related Controls	09/15	10	10	0	03/18	9	1

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Collecting Additional Information Can Help the CFPB Manage Its Future Space-Planning Activities	02/16	1	1	0	02/18	0	1
The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	0	12/17	2	7
2016 Audit of the CFPB's Information Security Program	11/16	3	3	0	10/17	1	2
The CFPB's Advisory Committees Help Inform Agency Activities, but Advisory Committees' Administration Should Be Enhanced	11/16	7	7	0	03/18	7	0
The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities	03/17	5	5	0	03/18	5	0
The CFPB Can Strengthen Contract Award Controls and Administrative Processes	03/17	6	6	0	01/18	6	0
Security Control Review of the CFPB's Active Directory Implementation (nonpublic report)	04/17	1	1	0	01/18	1	0

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information	05/17	9	9	0	03/18	6	3
Security Control Review of the CFPB's Public Website (nonpublic report)	05/17	8	8	0	01/18	2	6
The CFPB Can Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-job Training Program	09/17	9	9	0	03/18	3	6
The CFPB Generally Complies With Requirements for Issuing Civil Investigative Demands but Can Improve Certain Guidance and Centralize Recordkeeping	09/17	3	3	0	n.a.	2[a]	1
The CFPB Can Improve Its Examination Workpaper Documentation Practices	09/17	17	17	0	n.a.	0	17
2017 Audit of the CFPB's Information Security Program	10/17	7	7	0	n.a.	0	7
The CFPB Can Further Strengthen Controls Over Certain Offboarding Processes and Data	01/18	11	11	0	n.a.	0	11

See notes at end of table.

Report title	Issue date	Recommendations			Status of recommendations		
		Number	Mgmt. agrees	Mgmt. disagrees	Last follow-up date	Closed	Open
Report on the Independent Audit of the Consumer Financial Protection Bureau's Privacy Program	02/18	2	2	0	n.a.	0	2

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

n.a. not applicable.

a. These recommendations were closed when the report was issued.

Table A-5. Audit, Inspection, and Evaluation Reports Issued to the Board and the CFPB 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 CFPB 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	59
Investigations opened during the reporting period	13
Investigations closed during the reporting period	15
Investigations open at end of the period	57
Investigative results for the reporting period	
Persons referred to U.S. Department of Justice prosecutors	2
Persons referred to state/local prosecutors	1
Declinations received	5
Joint investigations	35
Reports of investigations issued	2
Oral and/or written reprimands	1
Terminations of employment	0
Arrests	0
Suspensions	0
Debarments	0
Prohibitions from banking industry	1
Indictments	1
Criminal informations	0
Criminal complaints	0
Convictions	1
Civil actions	$44,000,000

See notes at end of table.

Investigative actions	Number or dollar value[a]
Administrative monetary recoveries and reimbursements	$24,960
Civil judgments	$0
Criminal fines, restitution, and special assessments	$1,025,842
Forfeiture	$1,378,845

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	11
Complaints received during reporting period	412
Total complaints for reporting period	423
Complaints resolved during reporting period	401
Complaints pending	22

Appendix B: Inspector General Empowerment Act of 2016 Requirements

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

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

- See appendix C.

Statistical tables showing for the reporting period (1) the number of issued investigative reports, (2) the number of persons referred to the U.S. Department of Justice (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) a detailed description of the facts and circumstances of the investigation as well as the status and disposition of the matter, (2) whether the matter was referred to DOJ and the date of the referral, and (3) whether 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 CFPB to interfere with the independence of the OIG, including (1) through budget constraints designed to limit OIG capabilities and (2) incidents when the agency has resisted or objected to OIG oversight activities or restricted or significantly delayed OIG access to information, including the justification of the establishment for such action.

- We have no such attempts to report.

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

- We have no such instances to report.

Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations

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

Board of Governors of the Federal Reserve System

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

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2011	1	2
2012	1	1
2013	1	1
2014	3	5
2015	3	7
2016	4	23
2017	6	38
2018[a]	3	12

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, 2018.

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

June 13, 2011

Total number of recommendations: 2
Recommendations open: 2

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

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

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

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

March 30, 2012

Total number of recommendations: 8
Recommendations open: 1

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

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

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

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

Total number of recommendations: 1
Recommendations open: 1

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

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

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

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

Total number of recommendations: 3[4]
Recommendations open: 2

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

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

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

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

Opportunities Exist to Enhance the Board's Oversight of Future Complex Enforcement Actions

2014-SR-B-015 September 30, 2014

Total number of recommendations: 5
Recommendations open: 2

Our objectives for this evaluation were (1) to evaluate the Board's overall approach to oversight of the amended consent orders; (2) to determine the effectiveness of the Board's oversight of the borrower slotting process; and (3) to determine the effectiveness of the Board's oversight of the servicers' paying agent, Rust Consulting, Inc.

In February 2013, the Board and the OCC issued amended consent orders that require mortgage servicers to provide about $3.67 billion in payments to nearly 4.2 million borrowers based on possible harm and to provide other foreclosure prevention assistance. We found that the Board's advance preparation and planning efforts for the payment agreement with the 13 servicers that joined the agreement in January 2013 were not commensurate with the complexity associated with this unprecedented interagency effort. Further, we found that data integrity issues at two servicers affected the reliability and consistency of the slotting results. The approach to resolving these data integrity issues may have resulted in borrowers who experienced similar harm receiving different payment amounts.

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

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

Total number of recommendations: 3
Recommendations open: 1

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

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

Review of the Failure of Waccamaw Bank

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

Total number of recommendations: 5
Recommendations open: 2

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

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

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

Total number of recommendations: 3
Recommendations open: 3

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

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

Security Control Review of the Board's Statistics and Reserves System (nonpublic report)

2015-IT-B-021 **December 17, 2015**

Total number of recommendations: 6
Recommendations open: 2

We evaluated the adequacy of selected information security controls for protecting Board data in the Board's Statistics and Reserves System (STAR) from unauthorized access, modification, destruction, or disclosure, as well as the system's compliance with FISMA and the Board's information security policies, procedures, standards, and guidelines.

Overall, we found that the Board's Division of Monetary Affairs and Division of Information Technology had taken several steps to implement information security controls for STAR, in accordance with FISMA and the Board's information security program. However, we identified opportunities to improve the Board's security governance of STAR to ensure that information security controls are adequately implemented, assessed, authorized, and monitored.

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

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

Total number of recommendations: 9
Recommendations open: 1

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

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

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

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

Total number of recommendations: 10
Recommendations open: 9

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

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

2016 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 4

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

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

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

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

Total number of recommendations: 11
Recommendations open: 9

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

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

channels for System decisionmakers to be aware of supervision employees' divergent views about material issues regarding LISCC firms and LBOs.

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

The Board Can Improve Documentation of Office of Foreign Assets Control Examinations

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

Total number of recommendations: 2
Recommendations open: 2

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

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

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

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

Total number of recommendations: 2
Recommendations open: 2

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

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

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

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

Total number of recommendations: 8
Recommendations open: 8

We assessed (1) the Board's current cybersecurity oversight approach and governance structure, (2) the current examination practices for financial market utilities and multiregional data processing servicer (MDPS) firms for which the Board has oversight responsibilities, and (3) the Board's ongoing initiative for the future state of cybersecurity oversight. We found that the Division of Supervision and Regulation could improve the oversight of MDPS firms by (1) enforcing a reporting requirement in the Bank Service Company Act, (2) considering the implementation of an enhanced governance structure for these firms, (3) providing additional guidance on the supervisory expectations for these firms, and (4) ensuring that the division's intelligence and incident management function is aware of the technologies used by MDPS firms. We also identified opportunities to improve the recruiting, retention, tracking, and succession

planning of cybersecurity resources, as well as opportunities to enhance the internal communications about cybersecurity-related risks.

The Board Can Strengthen Its Guidance and Planning Efforts for Future Evaluations of the Law Enforcement Unit

2017-MO-B-013 **August 16, 2017**

Total number of recommendations: 3
Recommendations open: 3

We conducted an evaluation of the Board Internal Oversight Committee's (IOC) evaluation of the Law Enforcement Unit (LEU). Our objective was to assess the IOC's 2015 evaluation of the LEU's compliance with policies and procedures.

The IOC did not provide guidance to those who conducted the evaluation of the Board LEU on documenting the tasks performed or the basis for all conclusions. As a result, we could not fully assess the IOC's evaluation. We also found that the IOC did not have detailed written guidance to ensure that evaluations were consistently and effectively conducted. Additionally, the IOC had not finalized a plan for identifying and securing resources with the requisite background and expertise to conduct future evaluations.

2017 Audit of the Board's Information Security Program

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

Total number of recommendations: 9
Recommendations open: 9

See the summary in the body of this report.

The Board's Organizational Governance System Can Be Strengthened

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

Total number of recommendations: 14
Recommendations open: 14

See the summary in the body of this report.

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

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

Total number of recommendations: 3
Recommendations open: 3

See the summary in the body of this report.

Review of the Failure of Allied Bank

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

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

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

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

Total number of recommendations: 7
Recommendations open: 7

See the summary in the body of this report.

Consumer Financial Protection Bureau

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

Year	Number of reports with unimplemented recommendations	Number of unimplemented recommendations
2012	0	0
2013	1	2
2014	2	4
2015	2	2
2016	3	10
2017	6	40
2018[a]	2	13

Note. Because the CFPB 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, 2018.

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

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

Total number of recommendations: 14
Recommendations open: 2

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

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

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

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

Total number of recommendations: 4
Recommendations open: 3

We reviewed the information system security controls for the CFPB's cloud computing–based general support system.

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

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 CFPB 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 CFPB'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 CFPB's information security program was generally consistent with the requirements for continuous monitoring, configuration management, and incident response; however, we identified opportunities to strengthen these areas through automation and centralization.

The CFPB Can Enhance Its Diversity and Inclusion Efforts

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

Total number of recommendations: 17
Recommendations open: 1

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

We identified four areas of the CFPB's diversity and inclusion efforts that could be enhanced. First, diversity and inclusion training was not mandatory for CFPB employees, supervisors, and senior managers.

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

The CFPB Can Enhance Its Contract Management Processes and Related Controls

2015-FMIC-C-014 **September 2, 2015**

Total number of recommendations: 10
Recommendations open: 1

We assessed the CFPB's compliance with applicable laws, regulations, and CFPB policies and procedures related to contract management, as well as the effectiveness of the CFPB's internal controls related to contract management.

In general, we found the CFPB complied with applicable laws, regulations, and CFPB policies and procedures, although we noted that certain contract management controls could have been improved in 3 of 29 contracts in our sample. We also found that 32 of the 79 contractor performance evaluations required by the *Federal Acquisition Regulation* were overdue. Further, the Bureau of the Fiscal Service's Division of Procurement omitted a contract clause designed to clarify the OIG's access to contractor records from 1 of the 10 contracts we sampled for this purpose. Our report also noted that the CFPB's Office of Minority and Women Inclusion had not yet developed standards and procedures to ensure that minority-owned and women-owned businesses were considered for CFPB procurements, including procedures that enabled the CFPB to know whether contractors failed to make a good faith effort to include minorities and women in their workforce.

Collecting Additional Information Can Help the CFPB Manage Its Future Space-Planning Activities

2016-FMIC-C-002 **February 3, 2016**

Total number of recommendations: 1
Recommendations open: 1

We assessed the CFPB's short-term and long-term space planning to determine whether controls were in place to effectively manage the agency's space needs and associated costs.

We identified controls that the Office of Administrative Operations used to plan for CFPB headquarters office space. Because the CFPB determined it did not have leasing authority, the Office of Administrative Operations planned to continue to use the U.S. General Services Administration for its future space procurement needs. To provide the CFPB with office space that met its needs, the U.S. General Services Administration collected information to understand the CFPB's space requirements. Therefore, the CFPB could have benefited from implementing a process for consistently collecting, maintaining, and using space-planning information to manage evolving regional office space needs and associated costs.

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

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

Total number of recommendations: 9
Recommendations open: 7

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

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

2016 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 3
Recommendations open: 2

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

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

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

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

Total number of recommendations: 9
Recommendations open: 3

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

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

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

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

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

Total number of recommendations: 8
Recommendations open: 6

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

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

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

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

Total number of recommendations: 9
Recommendations open: 6

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

Although the CFPB has taken steps to enhance the ECP since its implementation in October 2014, we identified additional ways in which the agency could improve the program. First, some examiners appeared to be pursuing components of the ECP before being fully prepared. Second, some examiners did not appear to receive adequate training or developmental opportunities and exposure to certain CFPB internal processes before starting certain components of the ECP. Third, the CFPB did not have a formal method to evaluate and update the ECP. Fourth, the CFPB did not consistently communicate ECP

requirements to prospective employees. Fifth, the ECP policy should be updated to clarify when the 5-year time requirement for examiners' obtaining their commissioning begins.

Finally, the CFPB could enhance its implementation of the OJT program. Specifically, CFPB regions have not consistently implemented the OJT program, and examiners have not clearly understood the requirements, expectations, and purpose of the program.

The CFPB Generally Complies With Requirements for Issuing Civil Investigative Demands but Can Improve Certain Guidance and Centralize Recordkeeping

2017-SR-C-015 **September 20, 2017**

Total number of recommendations: 3
Recommendations open: 1

Our review determined whether the sampled civil investigative demands (CIDs) contained the procedural elements required by the Dodd-Frank Act, including, but not limited to, the presence of certain information such as notifications of purpose, return dates, and custodians.

We found that the CFPB generally complied with the procedural elements of section 1052(c) of the Dodd-Frank Act and with internal procedures when issuing the sampled CIDs, but the agency can improve its guidance for crafting notifications of purpose associated with CIDs. A noncompliant notification of purpose may limit the recipient's ability to understand the basis for requests and thereby heighten the risk that the CID may face a legal challenge. In the event of such a challenge, the CFPB's ability to obtain the information needed to enforce consumer financial protection laws could be delayed. Additionally, noncompliant notifications of purpose pose a reputational risk, potentially affecting interactions with CID recipients and other stakeholders. During the course of our review, the CFPB updated its internal policies to mitigate this potential risk.

We also found that the Office of the Executive Secretariat does not appear to maintain a complete record of all petitions and supporting documents and does not use a centralized repository to maintain CIDs and related documentation.

The CFPB Can Improve Its Examination Workpaper Documentation Practices

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

Total number of recommendations: 17
Recommendations open: 17

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

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

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

2017 Audit of the CFPB's Information Security Program

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

Total number of recommendations: 7
Recommendations open: 7

See the summary in the body of this report.

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: 11

See the summary in the body of this report.

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

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

Total number of recommendations: 2
Recommendations open: 2

See the summary in the body of this report.

Abbreviations

Board	Board of Governors of the Federal Reserve System
CFPB	Consumer Financial Protection Bureau
CID	civil investigative demand
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
C-SCAPE	Consolidated Supervision Comparative Analysis, Planning and Execution System
DATA Act	Digital Accountability and Transparency Act of 2014
DIF	Deposit Insurance Fund
Dodd-Frank Act	Dodd-Frank Wall Street Reform and Consumer Protection Act
DOJ	U.S. Department of Justice
ECP	Examiner Commissioning Program
FBI	Federal Bureau of Investigation
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
IG	Inspector General
IOC	Internal Oversight Committee
IPIA	Improper Payments Information Act of 2002, as amended
LBO	large banking organization
LEU	Law Enforcement Unit
LISCC	Large Institution Supervision Coordinating Committee
MDPS	multiregional data processing servicer
NRAS	National Remote Access Services
OCC	Office of the Comptroller of the Currency
OFAC	Office of Foreign Assets Control
OIG	Office of Inspector General
OJT	On-the-Job Training
OMB	Office of Management and Budget

RADAR	Risk Assessment, Data Analysis, and Research
STAR	Statistics and Reserves System
Treasury	U.S. Department of the Treasury

Office of Inspector General

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

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