

Office of Inspector General

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

Semiannual Report to Congress

April 1, 2017–September 30, 2017



Semiannual Report to Congress

April 1, 2017–September 30, 2017



Office of Inspector General

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

Message From the Inspector General



This year marks the 30th anniversary of the Office of Inspector General (OIG) for the Board of Governors of the Federal Reserve System (Board). Voluntarily established by former Federal Reserve Chairman Paul Volcker in July 1987, the OIG's responsibilities became statutorily established 1 year later as part of the Inspector General Act Amendments of 1988. In 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act also named our office the OIG for the Consumer Financial Protection Bureau (CFPB). The OIG has been expanding its presence and evolving ever since.

Beginning with just a handful of staff in the earliest days, the OIG now includes a headquarters location in Washington, DC, as well as four regional offices across the country. What has remained constant over the past 30 years is our commitment to providing independent oversight and promoting economy, efficiency, and effectiveness in the programs and operations of the agencies that we oversee.

During the current reporting period, we completed reviews of the Board in the areas of cybersecurity, management and operations, and financial management and internal controls. For the CFPB, we completed reviews in the areas of supervision and enforcement and information technology. In addition, we issued reports of the major management challenges facing both the Board and the CFPB. These reports help our agencies to identify areas that may hamper their ability to successfully accomplish their strategic objectives.

Our Office of Investigations has continued to investigate allegations of fraud, waste, and abuse related to the Board's and the CFPB's programs and operations and has had great success in bringing wrongdoers to justice. Over the past 6 months, we received 242 Hotline complaints, opened 16 new investigations, and closed 21 investigations. Our work resulted in 10 individuals referred for criminal prosecution; 6 indictments; over \$8 million in criminal fines, restitution, and special assessments; \$225 million in civil judgments; and a clear message to those involved in wrongdoing within or against the Board or the CFPB that they will be held accountable for their illegal activities.

In furtherance of our vision to be *the* trusted oversight organization of the Board and the CFPB, we have focused efforts on raising awareness about the OIG Hotline with our key partners in the fight against fraud, waste, and abuse. Our focus on outreach and the addition of Hotline links on agency intranets have resulted in nearly double the number of referrals as compared to previous years. We also continued to strengthen relationships with our law enforcement partners by hosting and attending conferences that drew attendees from dozens of federal, state, and local law enforcement agencies.

I am proud to be a part of the OIG's history and am confident that over the next 30 years, we will continue to rise to the challenge of carrying out our critical oversight role. I would like to express my appreciation to the OIG staff for their dedication, hard work, and unwavering commitment to our mission, vision, and values.

Sincerely,

A handwritten signature in black ink that reads "Mark Bialek". The signature is written in a cursive, flowing style.

Mark Bialek
Inspector General
October 31, 2017



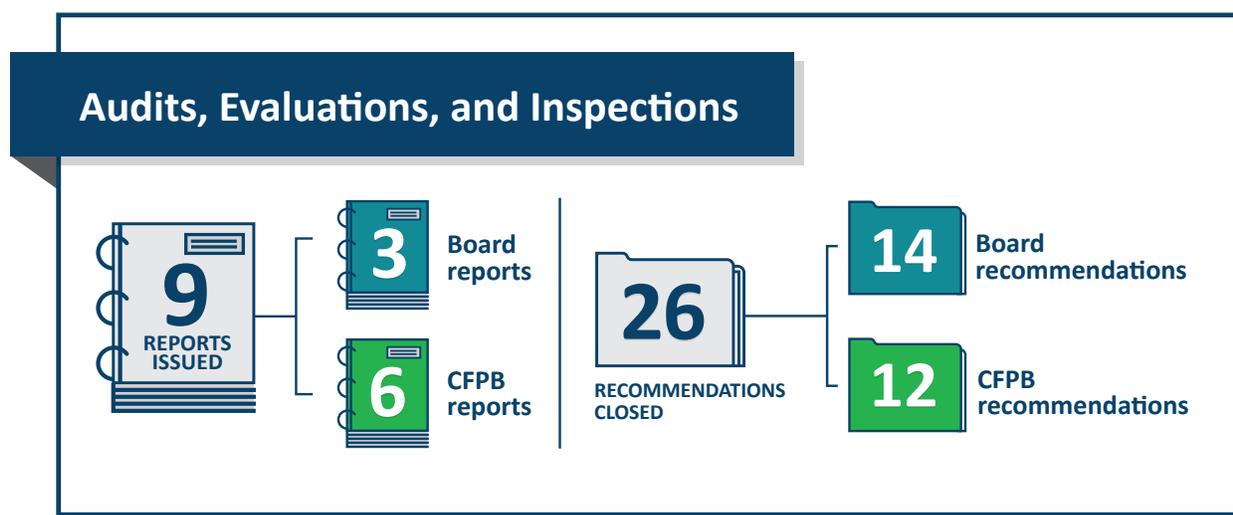
Contents

Highlights	1
Introduction	5
Major Management Challenges	9
Audits, Evaluations, and Inspections	11
Board of Governors of the Federal Reserve System	11
Consumer Financial Protection Bureau	13
Failed State Member Bank Reviews	19
Material Loss Reviews	19
Nonmaterial Loss Reviews	19
Investigations	21
Board of Governors of the Federal Reserve System	21
Consumer Financial Protection Bureau	23
Hotline	25
Legislative and Regulatory Review, Congressional and Media Activities, and CIGIE Participation	27
Legislative and Regulatory Review	27
Congressional and Media Activities	28
CIGIE Participation	28
Peer Reviews	29
Appendix A: Statistical Tables	31
Appendix B: Inspector General Empowerment Act of 2016 Requirements	45
Appendix C: Summaries of Reports With Outstanding Unimplemented Recommendations	47

Board of Governors of the Federal Reserve System	47
Consumer Financial Protection Bureau	59
Abbreviations	69

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 Approach to Cybersecurity Supervision

The Board can enhance its approach to cybersecurity supervision as it implements its multiyear cybersecurity oversight program.

The CFPB's Examination Workpaper Documentation Practices

The CFPB can improve its approach to documenting examination results and protecting sensitive information so that only employees with a business need have access to materials with confidential supervisory information and personally identifiable information.

The CFPB's Examiner Commissioning Program

The CFPB can improve the design, implementation, and execution of its Examiner Commissioning Program and On-the-Job Training program to ensure that its examiners are fully prepared before pursuing commissioning and that the Examiner Commissioning Program is evaluated and updated as needed.

The Board’s Martin Building Project

Although the Board’s controls over contracted architectural and engineering services are designed effectively and communication channels help the project team, the Board can strengthen its internal controls and communication as the Martin Building project progresses.

The CFPB’s Issuance of Civil Investigative Demands

Although the CFPB generally complied with the procedural elements of section 1052(c) of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and with its own procedures when issuing the civil investigative demands in our sample, the agency can improve its guidance for crafting notifications of purpose associated with civil investigative demands.



Former Acting President of CFG Community Bank Indicted

A former acting President of CFG Community Bank was charged in an indictment with one or more counts of bank fraud, theft by a bank officer, conspiracy to defraud the United States, and tax evasion. Another subject was charged with conspiracy to defraud the United States and tax evasion. The indictment alleged that over \$875,000 of the bank's loan proceeds was diverted to the former acting President's personal benefit or to the benefit of a friend.

Former President and Chief Executive Officer of Farmers Exchange Bank Pleaded Guilty to Bank Fraud, False Entries, and False Statements

The former President and Chief Executive Officer of Farmers Exchange Bank in Neshkoro, Wisconsin, pleaded guilty to three counts of bank fraud; one count of false entries, reports, and transactions; and one count of false statements. The defendant also signed a stipulation and settlement agreement, in which he agreed that the \$338,000 seized from his bank accounts pursuant to a seizure warrant, which were monies derived from proceeds of traceable theft, embezzlement, or misapplication of funds by a bank holding company officer, would be paid to the other shareholders of FEB Bancshares, Inc.



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 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.
- The Federal Information Security Modernization Act of 2014 (FISMA; 44 U.S.C. § 3555) established a legislative mandate for ensuring the effectiveness of information security controls over resources that support federal operations and assets. In accordance with FISMA requirements, we perform annual independent reviews of the Board's and the 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 Federal Deposit Insurance Corporation, the Federal Housing Finance Agency, the National Credit Union Administration, the U.S. Securities and Exchange Commission, and the Office of the Special Inspector General for the Troubled Asset Relief Program.

2. The FFIEC is a formal interagency body empowered (1) to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board, the Federal Deposit Insurance Corporation, the National Credit Union Administration, the Office of the Comptroller of the Currency, and the 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. 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.



Major Management Challenges

Although not required by statute, we annually report on the major management challenges facing the Board and the CFPB. These challenges identify the areas that, if not addressed, are most likely to hamper the Board's and the CFPB's accomplishment of their strategic objectives. The agencies' 2017 challenges closely track those for 2016.

For 2017, we identified five major management challenges for the Board:

- Enhancing Governance, Including Using an Enterprise Approach to Carry Out Agencywide Functions
- Enhancing Oversight of Cybersecurity at Supervised Financial Institutions
- Ensuring an Effective Information Security Program
- Continuing to Strengthen the Regulatory and Supervisory Framework While Remaining Sufficiently Nimble to Address Potential Internal or External Developments
- Managing the Handling and Release of Sensitive Federal Open Market Committee and Board-Generated Information

For 2017, we identified four major management challenges for the CFPB:

- Ensuring an Effective Information Security Program
- Maturing the Human Capital Program
- Strengthening the System of Internal Controls
- Effectively Managing and Acquiring Workspace

See our website for our full [management challenges memorandums](#) to the Board and the CFPB.



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.

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

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

We assessed the Board’s cybersecurity examination approach to determine whether it is providing effective oversight of financial institutions’ information security controls and cybersecurity risks for select oversight areas. Specifically, this evaluation included an assessment of (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 identified opportunities for the Division of Supervision and Regulation to enhance its approach to cybersecurity supervision as it continues to implement its multiyear, future-state cybersecurity oversight program. Specifically, we found that the Division of Supervision and Regulation could improve the oversight of MDPS firms by (1) enforcing the reporting requirement in the Bank Service Company Act for financial institutions to notify their primary regulator of new service relationships within 30 days, (2) considering the implementation of an enhanced governance structure for these firms, (3) providing additional guidance to examination teams 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. Further, we identified opportunities to improve the recruiting, retention, tracking, and succession planning of cybersecurity resources in alignment with the Board’s strategic plan, as well as opportunities to enhance the internal communications about cybersecurity-related risks.

Our report contains recommendations designed to enhance several components of the Division of Supervision and Regulation’s approach to cybersecurity supervision. The Board concurred with our recommendations.

The Board Can Improve Communication and Documentation Regarding the Martin Building Project

2017-FMIC-B-012

May 24, 2017

We assessed the effectiveness of the Board’s controls over contracted architecture and engineering services for the Martin Building renovation project. The initial architecture and engineering services contract was canceled in 2015, and the Martin Building project’s time frame has been extended. As of March 2017, the Board expected construction to be completed in the fourth quarter of 2019, with move-in scheduled for the first quarter of 2020. Given the cost, complexity, and time remaining until expected completion, we undertook this audit to identify lessons learned and opportunities for the Board to improve its contract management for the Martin Building project going forward.

We found that the Board’s controls over contracted architecture and engineering services were designed effectively and communication channels were established to help the project team manage the Martin Building project. However, the project team’s communication with and documentation provided to the Chief Operating Officer and the Executive Oversight Group could have been improved to better reflect the Martin Building renovation’s progress, particularly during the schematic design phase. Documentation of key discussion topics, advice, decisions, or recommendations made by the Executive Oversight Group could also be improved. Further, we identified other matters regarding contract management

for consideration going forward to better manage contractor performance and to reduce the risk of unplanned costs.

Our report contains recommendations designed to strengthen the Board’s internal controls and communication during the Martin Building renovation project. The Board concurred with our recommendations.

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

2017-MO-B-013

August 16, 2017

As part of our external oversight function duties for the Board’s Law Enforcement Unit (LEU), we conducted an evaluation of the Board Internal Oversight Committee’s (IOC) evaluation of the LEU. Our objective was to assess the Board IOC’s 2015 evaluation of the LEU’s compliance with the *Uniform Regulations for Federal Reserve Law Enforcement Officers* and internal policies and procedures.

We found that the IOC did not provide the individuals who conducted the October 2015 evaluation of the Board LEU with guidance on documenting the testing performed or the basis for all conclusions. As a result, we did not have sufficient documentation to fully assess the IOC’s evaluation of the LEU’s compliance with the *Uniform Regulations for Federal Reserve Law Enforcement Officers* and internal policies and procedures. 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.

Our report contains recommendations to improve the IOC’s evaluation process. Our recommendations are designed to help ensure that evaluations are thoroughly documented and consistently conducted and that appropriate resources are available for future reviews. The Board generally concurred with our recommendations.

Consumer Financial Protection Bureau

Security Control Review of the CFPB’s Active Directory Implementation

2017-IT-C-008

April 17, 2017

As part of our FISMA mandate, we conducted this audit to evaluate the administration and security design effectiveness of the CFPB’s Active Directory implementation, including the adequacy of selected security controls for protecting Active Directory, as well as the system’s compliance with FISMA and

the information security policies, procedures, standards, and guidelines of the CFPB. Active Directory is used to store information about resources on the network and to provide a means to centrally organize, manage, and control access to those resources. Active Directory is hosted within a third-party private cloud environment.

Overall, we found that the CFPB was effectively administering and protecting its Active Directory implementation; however, the CFPB could strengthen Active Directory controls in the areas of identity and access management and risk management. In addition, as noted in our [2016 Audit of the CFPB's Information Security Program](#) report, improvements were still needed in the management of access agreements for Active Directory users.

Our report includes one recommendation and one item for management's consideration. The CFPB concurred.

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

2017-SR-C-011

May 15, 2017

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 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.

In addition, we found that the Office of Enforcement did not follow specific aspects of the document labeling and storage requirements contained in the CFPB's standards 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.

Our report contains recommendations designed to improve the Office of Enforcement's practices for managing and safeguarding confidential investigative information. The CFPB concurred with our recommendations.

Security Control Review of the CFPB’s Public Website

2017-IT-C-010

May 22, 2017

As part of our FISMA mandate, 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. If not addressed, these deficiencies could adversely affect the confidentiality, integrity, and availability of consumerfinance.gov and the information it contains. We also identified additional risks for management’s continued attention. Those risks relate to system and communications protection, audit and accountability, identification and authentication, system and information integrity, and configuration management.

Our report includes recommendations designed to strengthen the security of consumerfinance.gov. The CFPB concurred with our recommendations.

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

We assessed the CFPB’s adherence to its policies and procedures for issuing civil investigative demands (CIDs) and its general compliance with the requirements in section 1052(c) of the Dodd-Frank Act. Specifically, our review determined whether the sampled 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. During our review, we learned that in accordance with internal guidance, a CID’s notification of purpose is identical to the statement of purpose in the associated investigation’s opening memorandum, which may be revised later in the investigation. Internal guidance calls for broad statements of purpose, to allow for flexibility. The guidance does not expressly remind enforcement attorneys of the need for statements of purpose to be compliant with relevant case law on notifications of purpose, including any developments in such case law, or remind

them to revisit the statement of purpose in a revised opening memorandum if the purposes of the investigation evolve. A potentially 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, irrespective of the court’s decision. 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 CFPB can improve its matter management system. Specifically, we found that the Office of the Executive Secretariat does not appear to maintain a complete record of all petitions and supporting documents. In addition, the Office of Enforcement does not use a centralized repository to maintain CIDs and related documentation; rather, the agency maintains CID documentation on the shared drives of multiple offices.

Our report contains a recommendation to improve the Office of Enforcement’s practices for crafting notifications of purpose for CIDs to reduce the risk that notifications of purpose may result in legal challenges from CID recipients. Our report also contains recommendations for the agency to implement a centralized matter management system to ensure that official federal records are easily retrievable. The CFPB concurred with our recommendations.

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

2017-SR-C-014

September 20, 2017

We evaluated the effectiveness of the CFPB’s management of the Examiner Commissioning Program (ECP) and the On-the-Job Training (OJT) program. As part of this evaluation, we assessed the programs’ design, implementation, and execution.

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.

Our report contains recommendations designed to enhance the effectiveness of the CFPB’s ECP and OJT program. The CFPB concurred with our recommendations.

The CFPB Can Improve Its Examination Workpaper Documentation Practices

2017-SR-C-016

September 27, 2017

We assessed the CFPB’s guidance and practices to promote effective and consistent examination workpaper documentation. Specifically, 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 (SEFL) approach was to grant examination employees in each region open access to all examination workpaper documentation and supporting materials in the initial system of record and on the current shared drive for examinations conducted in that region. One region used a similar open-access approach for the prior shared drive. This approach resulted in certain SEFL 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.

In addition, we found that file size limitations in the initial system of record led examiners to store workpapers in multiple locations. We also found opportunities to reinforce the need to store workpapers in the appropriate location and to document supervisory reviews and sampling methods. Further, we recommended that SEFL develop workpaper training and an ongoing quality review process.

Our report contains recommendations designed to improve SEFL’s approach to documenting examination results and protecting sensitive information. We acknowledge that SEFL management has acted to address some of the issues discussed in this report, but we have not tested these actions to determine whether they fully address our recommendations. The CFPB concurred with our recommendations.



Failed State Member Bank Reviews

Material Loss Reviews

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

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

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

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

Nonmaterial Loss Reviews

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

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

The IG must semiannually report the completion dates for each such review. If an in-depth review is not warranted, the IG is required to explain this determination. In general, we consider a loss to the DIF to present unusual circumstances if the conditions associated with the bank's deterioration, ultimate closure,

and supervision were not addressed in any of our prior bank failure reports, or if there was potential fraud.

We completed our initial review of the Fayette County Bank failure and identified a series of unusual circumstances that warrant an in-depth review (table 1). 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
Fayette County Bank	St. Elmo, Illinois	\$34.4	\$10	05/26/2017	Unsafe and unsound condition	Circumstances warrant an in-depth review



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

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 holding company directors or officers 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 Acting President of CFG Community Bank Indicted

A former acting President of CFG Community Bank was charged in an indictment with one or more counts of bank fraud, theft by a bank officer, conspiracy to defraud the United States, and tax evasion. Another subject was charged with conspiracy to defraud the United States and tax evasion.

The indictment alleged that the former acting President of the Board-supervised state member bank devised a scheme to defraud the bank by refinancing bank-owned mortgage loans. Over \$875,000 of the bank's loan proceeds was diverted, at the direction of the former acting President and using false documents, to the former acting President's personal benefit or to the benefit of a friend.

This was a joint investigation by the Federal Bureau of Investigation (FBI), Internal Revenue Service (IRS)–Criminal Investigation, the Social Security Administration OIG, and our office, with prosecutorial support from the U.S. Attorney's Office for the District of Maryland.

Former President and Chief Executive Officer of Farmers Exchange Bank Pleaded Guilty to Bank Fraud, False Entries, and False Statements

The former President and Chief Executive Officer of Farmers Exchange Bank in Neshkoro, Wisconsin, pleaded guilty in U.S. District Court for the Eastern District of Wisconsin to three counts of bank fraud; one count of false entries, reports, and transactions; and one count of false statements. The defendant also signed a stipulation and settlement agreement in which he agreed that the \$338,000 seized from his bank accounts pursuant to a seizure warrant, which were monies derived from proceeds of traceable theft, embezzlement, or misapplication of funds by a bank holding company officer, would be paid to the other shareholders of FEB Bancshares, Inc.

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 FBI, with prosecutorial support from the U.S. Attorney's Office for the Eastern District of Wisconsin.

Multiple Former Pierce Commercial Bank Officials Sentenced for Conspiracy and Bank Fraud

A former Loan Officer of failed Pierce Commercial Bank was sentenced to 30 days of home detention, 100 hours of community service, 2 years of supervised release, and more than \$131,000 in restitution after pleading guilty to making false statements on loan applications. Four more former officials—two Vice Presidents, a Senior Loan Processor, and another Loan Officer—were sentenced to time served (1 day), 3 years' supervised release, and a \$100 special assessment for conspiracy to make false statements on loan applications and to commit bank fraud. All individuals were sentenced in the Western District of Washington in Tacoma.

Pierce Commercial Bank was a state member bank regulated by the Board. From 2004 to 2008, prior to its failure, the coconspirators and others at the bank solicited individuals, regardless of whether they were qualified, to apply for Pierce Commercial Bank home loans. The coconspirators then prepared uniform residential loan applications based on fraudulent representations with or without the borrowers' knowledge. The fraudulent scheme resulted in over 5,000 mortgage loans representing over \$1 billion in loan proceeds. Hundreds of borrowers involved in the scheme defaulted on their loans, resulting in over \$9.5 million in losses to Pierce Commercial Bank, secondary investors, the U.S. Department of Housing and Urban Development, and the U.S. Federal Housing Administration and \$24.8 million in losses to the DIF. The scheme contributed to the failure of the bank.

This investigation was conducted by the U.S. Attorney's Office for the Western District of Washington, the FBI, the U.S. Department of Housing and Urban Development OIG, the Federal Housing Finance Agency OIG, our office, the FDIC OIG, the Special Inspector General for the Troubled Asset Relief Program, and IRS–Criminal Investigation.

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.

Multiple 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, mail fraud, wire fraud, telemarketing fraud, conspiracy to commit money laundering, and money laundering in an alleged scheme to market and sell home loan modification services under the guise of a law firm. During sentencing, the co-owner of the loan modification company was sentenced to 84 months' imprisonment and 36 months' supervised release and was ordered to pay \$590,130 in restitution and a \$200 special assessment. A second individual, a Sales Manager, was sentenced to 24 months' supervised release and was ordered to pay a \$25 special assessment. The other co-owner and two other Sales Managers are awaiting sentencing.

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, IRS–Criminal Investigation, the Special Inspector General for the Troubled Asset Relief Program, and the Federal Housing Finance Agency OIG, with prosecutorial support from the U.S. Attorney's Office for the District of Utah.



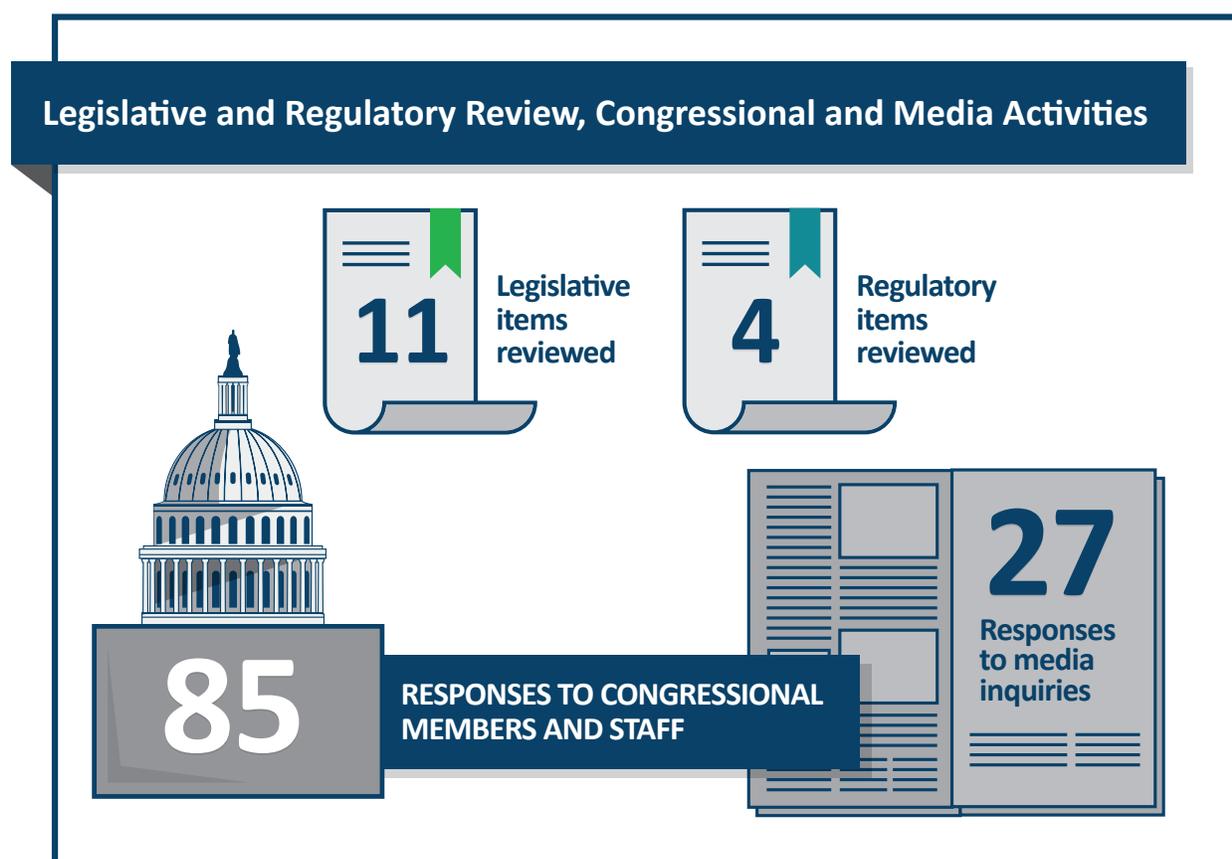
Hotline

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 Hotline received 242 complaints.

The OIG Hotline 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, 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, the OIG investigates 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 11 legislative items and 4 regulatory items.

Congressional and Media Activities

We communicate and coordinate with various congressional committees on issues of mutual interest. During this reporting period, we provided 85 responses to congressional members and staff concerning the Board and the CFPB. Additionally, we responded to 27 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’re 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 5,500 reports, detailing for fiscal year 2017 alone over \$26 billion in potential savings and 7,500 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 Assistant 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 August 2017, we completed a review of the system of internal safeguards and management procedures for the investigative operations of the OIG for the Export-Import Bank of the United States. In our opinion, the system of internal safeguards and management procedures for the investigative function of the OIG for the Export-Import Bank of the United States in effect for the period ending June 30, 2017, was in compliance with the quality standards established by CIGIE and the applicable Attorney General guidelines. These safeguards and procedures provide the OIG for the Export-Import Bank of the United States with reasonable assurance of conformance with professional standards in the planning, execution, and reporting of its investigations.
- 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
The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing	Evaluation
The Board Can Improve Communication and Documentation Regarding the Martin Building Project	Audit
The Board Can Strengthen Its Guidance and Planning Efforts for Future Evaluations of the Law Enforcement Unit	Evaluation
Total number of audit reports: 1	
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	–	09/17	–	2
Evaluation of Prompt Regulatory Action Implementation	09/11	1 ^a	1	–	09/17	–	1
Security Control Review of the National Remote Access Services System (nonpublic report)	03/12	8	8	–	09/16	7	1
Security Control Review of the Board’s Public Website (nonpublic report)	04/12	12	12	–	05/16	9	3
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	–	09/17	1	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
The Board Can Benefit from Implementing an Agency-Wide Process for Maintaining and Monitoring Administrative Internal Control	09/13	1	1	–	02/17	–	1
Enforcement Actions and Professional Liability Claims Against Institution-Affiliated Parties and Individuals Associated with Failed Institutions	07/14	3 ^a	3	–	09/17	1	2
Opportunities Exist to Enhance the Board’s Oversight of Future Complex Enforcement Actions	09/14	5	5	–	09/17	3	2
Opportunities Exist to Improve the Operational Efficiency and Effectiveness of the Board’s Information Security Life Cycle	12/14	3	3	–	03/17	2	1
Review of the Failure of Waccamaw Bank	03/15	5	5	–	08/17	3	2

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
Security Control Review of the Board’s Consolidated Supervision Comparative Analysis, Planning and Execution System (nonpublic report)	09/15	3	3	–	–	–	3
2015 Audit of the Board’s Information Security Program	11/15	4	4	–	11/16	3	1
Security Control Review of the Board’s Statistics and Reserves System (nonpublic report)	12/15	6	6	–	–	–	6
The Board Should Strengthen Controls to Safeguard Embargoed Sensitive Economic Information Provided to News Organizations	04/16	9	9	–	09/17	8	1
Security Control Review of the Board’s Active Directory Implementation (nonpublic report)	05/16	10	10	–	–	–	10
2016 Audit of the Board’s Information Security Program	11/16	9	9	–	–	–	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
Opportunities Exist to Increase Employees' Willingness to Share Their Views About Large Financial Institution Supervision Activities	11/16	11	11	–	09/17	2	9
The Board Can Improve Documentation of Office of Foreign Assets Control Examinations	03/17	2	2	–	–	–	2
The Board Can Improve the Effectiveness of Continuous Monitoring as a Supervisory Tool	03/17	2	2	–	09/17	–	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	–	–	–	8
The Board Can Improve Communication and Documentation Regarding the Martin Building Project	05/17	3	3	–	09/17	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
The Board Can Strengthen Its Guidance and Planning Efforts for Future Evaluations of the Law Enforcement Unit	08/17	3	3	–	–	–	3

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

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
Security Control Review of the CFPB's Active Directory Implementation	Audit
The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information	Evaluation
Security Control Review of the CFPB's Public Website	Audit
The CFPB Generally Complies With Requirements for Issuing Civil Investigative Demands but Can Improve Certain Guidance and Centralize Recordkeeping	Evaluation
The CFPB Can Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-Job Training Program	Evaluation
The CFPB Can Improve Its Examination Workpaper Documentation Practices	Evaluation
Total number of audit reports: 2	
Total number of evaluation reports: 4	

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
Evaluation of the Consumer Financial Protection Bureau's Consumer Response Unit	09/12	5	5	–	09/17	5	–
The CFPB Should Strengthen Internal Controls for Its Government Travel Card Program to Ensure Program Integrity	09/13	14	14	–	03/17	11	3
The CFPB Has Established Effective GPRA Processes, but Opportunities Exist for Further Enhancement	06/14	3	3	–	08/17	3	–
Security Control Review of the CFPB's Cloud Computing–Based General Support System (nonpublic report)	07/14	4	4	–	09/16	1	3
Audit of the CFPB's Acquisition and Contract Management of Select Cloud Computing Services	09/14	4	4	–	09/16	3	1
2014 Audit of the CFPB's Information Security Program	11/14	3	3	–	11/16	2	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
The CFPB Can Enhance Its Diversity and Inclusion Efforts	03/15	17	17	–	09/17	14	3
The CFPB Can Enhance Its Contract Management Processes and Related Controls	09/15	10	10	–	02/17	9	1
Opportunities Exist to Enhance Management Controls Over the CFPB’s Consumer Complaint Database	09/15	8	8	–	06/17	8	–
Collecting Additional Information Can Help the CFPB Manage Its Future Space-Planning Activities	02/16	1	1	–	02/17	–	1
The CFPB Should Continue to Enhance Controls for Its Government Travel Card Program	06/16	9	9	–	03/17	1	8
2016 Audit of the CFPB’s Information Security Program	11/16	3	3	–	–	–	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
The CFPB's Advisory Committees Help Inform Agency Activities, but Advisory Committees' Administration Should Be Enhanced	11/16	7	7	–	09/17	5	2
The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities	03/17	5	5	–	–	3 ^a	2
The CFPB Can Strengthen Contract Award Controls and Administrative Processes	03/17	6	6	–	–	–	6
Security Control Review of the CFPB's Active Directory Implementation (nonpublic report)	04/17	1	1	–	–	–	1
The CFPB Can Improve Its Practices to Safeguard the Office of Enforcement's Confidential Investigative Information	05/17	9	9	–	09/17	3	6
Security Control Review of the CFPB's Public Website (nonpublic report)	05/17	8	8	–	–	–	8

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 Enhance the Effectiveness of Its Examiner Commissioning Program and On-the-job Training Program	09/17	9	9	–	–	–	9
The CFPB Generally Complies With Requirements for Issuing Civil Investigative Demands but Can Improve Certain Guidance and Centralize Recordkeeping	09/17	3	3	–	–	2 ^a	1
The CFPB Can Improve Its Examination Workpaper Documentation Practices	09/17	17	17	–	–	–	17

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.

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	64
Investigations opened during the reporting period	16
Investigations closed during the reporting period	21
Investigations open at end of the period	59
Investigative results for the reporting period	
Persons referred to U.S. Department of Justice prosecutors	10
Persons referred to state/local prosecutors	0
Declinations received	9
Joint investigations	34
Reports of investigations issued	2
Oral and/or written reprimands	0
Terminations of employment	0
Arrests	2
Suspensions	0
Debarments	0
Prohibition from banking industry	4
Indictments	6
Criminal informations	5
Criminal complaints	0
Convictions	8
Civil actions	0
Administrative monetary recoveries and reimbursements	\$0

See notes at end of table.

Investigative actions	Number or dollar value^a
Civil judgments	\$225,000,000
Criminal fines, restitution, and special assessments	\$8,409,394

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	20
Complaints received during reporting period	242
Total complaints for reporting period	262
Complaints resolved during reporting period	251
Complaints pending	11



Appendix B: Inspector General Empowerment Act of 2016 Requirements

The Inspector General Empowerment Act of 2016 amends 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 new 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.

- 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.

- In September 2015, we completed the survey phase for an information technology audit of the Board's data governance program. We learned that the program was not fully developed, and we postponed the audit. At that time, we anticipated revisiting the audit in the third quarter of 2016; however, on learning that a management and operations review of the program would produce more-meaningful results than an information technology audit, we closed the audit in May 2017. We plan to review this program from a management and operations perspective in the future.
- We initiated an investigation concerning allegations that a Board employee engaged in retaliatory behavior. The allegation was unsubstantiated. Per standard practice, the matter was presented to DOJ on January 30, 2017, which declined prosecution. The employee subsequently resigned. This investigation was closed. (case I20160045)



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	2	3
2012	2	4
2013	2	2
2014	3	5
2015	4	12
2016	4	29
2017 ^a	4	15

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

a. Through September 30, 2017.

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.

Evaluation of Prompt Regulatory Action Implementation

FRB OIG 2011-05

September 30, 2011

Total number of recommendations: 1³

Recommendations open: 1

We, the FDIC OIG, and the Treasury OIG conducted a review of the prompt regulatory action (PRA) provisions of the Federal Deposit Insurance Act. Our work focused on the following objectives:

3. This recommendation was directed jointly to the OCC, the FDIC, and the Board.

- determining the purpose of and circumstances that led to the PRA provisions (Federal Deposit Insurance Act sections 38 and 39) and lessons learned from the savings and loan crisis in the 1980s
- evaluating to what extent prompt corrective action and the safety and soundness standards were factors in bank failures and problem institutions during the current crisis
- assessing whether these provisions prompted federal regulators to act more quickly and more forcefully to limit losses to the DIF, in light of findings and lessons learned from the savings and loan crisis and regulators' use of PRA provisions in the current crisis
- determining whether there were other noncapital measures that provided a leading indication of risks to the DIF that should have been considered as part of the PRA provisions

We found that PRA provisions were appropriately implemented and helped strengthen oversight to a degree.

To improve the effectiveness of the PRA framework and to meet the section 38 and 39 goals of identifying problems early and minimizing losses to the DIF, we recommended that the FDIC, Board, and OCC agency heads review the matters for consideration presented in this report and work through the Financial Stability Oversight Council to determine whether the PRA legislation or implementing regulations should be modified.

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 our 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.

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

April 20, 2012

Total number of recommendations: 12

Recommendations open: 3

Our audit objective was to evaluate the adequacy of selected security controls for protecting the Board’s public website application from unauthorized access, modification, destruction, or disclosure.

Our review showed that, in general, controls were adequately designed and implemented. However, we identified opportunities to strengthen information security controls to help ensure that the Board’s public website meets FISMA requirements.

Board Should Enhance Compliance with Small Entity Compliance Guide Requirements Contained in the Small Business Regulatory Enforcement Fairness Act of 1996

2013-AE-B-008

July 1, 2013

Total number of recommendations: 2

Recommendations open: 1

We assessed the Board’s compliance with certain requirements of the Small Business Regulatory Enforcement Fairness Act of 1996, as amended. We initiated this evaluation to determine the validity of a complaint received by the OIG Hotline concerning the Board’s compliance with the act.

We found that the Board was not consistent in developing or updating small entity compliance guides in accordance with the act’s requirements. In addition, the Board’s compliance guides did not consistently provide clear guidance to small entities explaining how to comply with certain rules or when the requirements of the specific rules would be satisfied. Instead, many of the guides merely restated and summarized each section of the rules.

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: 3⁴

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 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.

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.

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 the Office of Management and Budget. However, we identified opportunities to improve the operational efficiency and effectiveness of the Board’s management of its information security life cycle.

Review of the Failure of Waccamaw Bank

2015-SR-B-005

March 26, 2015

Total number of recommendations: 5

Recommendations open: 2

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

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

2015-IT-B-015

September 2, 2015

Total number of recommendations: 3

Recommendations open: 3

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

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

2015 Audit of the Board’s Information Security Program

2015-IT-B-019

November 13, 2015

Total number of recommendations: 4

Recommendations open: 1

We evaluated (1) the Board’s compliance with FISMA and related information security policies, procedures, standards, and guidance and (2) the effectiveness of security controls and techniques for a subset of the Board’s information systems.

Overall, we found that the Board’s Chief Information Officer had developed, documented, and implemented an information security program that was generally consistent with the requirements established by FISMA and the 10 areas outlined in the U.S. Department of Homeland Security’s FISMA reporting guidance for IGs. We made recommendations to improve the Board’s information security program in the areas of information security continuous monitoring, configuration management, and identity and access management.

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: 6

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: 10

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: 9

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 Regulation⁵ 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 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

See the [summary](#) in the body of this report.

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

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	3
2014	3	5
2015	2	4
2016	4	14
2017 ^a	8	50

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 September 30, 2017.

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: 3

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.

Audit of the CFPB’s Acquisition and Contract Management of Select Cloud Computing Services

2014-IT-C-016

September 30, 2014

Total number of recommendations: 4

Recommendations open: 1

We reviewed the CFPB’s acquisition and contract management for two of the CFPB’s seven cloud service providers to determine whether requirements for security, service levels, and access to records were planned for, defined in contracts, and monitored.

Overall, we found that (1) the CFPB’s contracts for cloud computing services included roles and responsibilities, information security requirements, and service-level expectations; (2) the CFPB had established a process to monitor both contractual and service-level requirements for its cloud service providers; and (3) the agency collected and maintained nondisclosure agreements from contractor personnel to protect sensitive information. However, we identified opportunities for improvement in the procurement and use of cloud services, such as performing alternatives analysis and cost analysis and including clauses that provide the access needed for electronic discovery and performing investigations. We also found that one of the contracts we reviewed did not (1) include a clause granting the OIG the right to examine agency records or (2) detail specific penalties or remedies for noncompliance with contract terms and service levels.

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. Although we found that the CFPB’s information security program was generally consistent with the requirements for continuous monitoring, configuration management, and incident response, 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: 3

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: 8

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: 3

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 CFPB's 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’s Advisory Committees Help Inform Agency Activities, but Advisory Committees’ Administration Should Be Enhanced

2016-MO-C-016

November 30, 2016

Total number of recommendations: 7

Recommendations open: 2

We audited CFPB activities related to its four advisory committees, which provide expert advice on specific issues related to the CFPB’s mission. Our objectives were (1) to assess the CFPB’s compliance with applicable laws and regulations related to advisory committees, (2) to assess the CFPB’s administration of the advisory committees, and (3) to evaluate the CFPB’s advisory committees’ effectiveness in informing the CFPB’s activities.

Overall, we found that the CFPB advisory committees were generally effective and operating in compliance with applicable laws and regulations for the period we reviewed. We also found that the CFPB should have improved its administration of advisory committee activities. Specifically, the Office of Advisory Board and Councils and the Office of Research could have improved their administrative processes by formally tracking the clearance process of documents before dissemination to advisory committee members, determining an optimal method to identify conflict of interests for certain members, retaining application materials, posting summaries of advisory committee meetings to the CFPB’s Advisory groups webpage, and centrally retaining advisory committee expenditure information. In addition, we found that assessing advisory committee effectiveness could have assisted the CFPB in determining whether the committees provide the agency with information and perspectives that help inform agency activities.

The CFPB Can Strengthen Its Controls for Identifying and Avoiding Conflicts of Interest Related to Vendor Activities

2017-SR-C-004

March 15, 2017

Total number of recommendations: 5

Recommendations open: 2

We assessed whether the CFPB effectively mitigates the risk of potential conflicts of interest associated with using vendors to support fair lending compliance and enforcement analysis. We focused on a contract for fair lending enforcement analysis and expert witness services.

We found that the CFPB could have strengthened its controls for identifying and avoiding potential conflicts of interest by (1) ensuring that vendors comply with existing documentation requirements; (2) clarifying roles and responsibilities; and (3) better facilitating vendor disclosure of potential conflicts, or affirmation that no conflicts exist, at the issuance of each task order. In addition, we found that the

CFPB should have evaluated the potential costs and benefits of performing more fair lending enforcement analysis internally.

The CFPB Can Strengthen Contract Award Controls and Administrative Processes

2017-FMIC-C-007

March 30, 2017

Total number of recommendations: 6

Recommendations open: 6

We assessed the CFPB’s compliance with the *Federal Acquisition Regulation* and CFPB policy related to the contract solicitation, selection, and award processes, as well as the effectiveness of the CFPB’s associated internal controls.

We found the CFPB was generally compliant with applicable laws, regulations, and CFPB policies and procedures related to contract preaward and award process controls. We noted, however, that on some occasions, reviews and approvals were overlooked or not documented as required by the *Federal Acquisition Regulation* or CFPB policy. The Procurement Office could have improved its contract file documentation by consistently including evidence that acquisition planning documents have been reviewed and approved and that conflict of interest documents for evaluation team members have been signed. The CFPB also could have improved the documentation used to support price reasonableness determinations for sole-source contracts and improved Routing and Review Slip documentation. We also found opportunities to expand the use of digital signatures in the acquisition process. Lastly, the Procurement Office could have captured and monitored acquisition lead-time data as a performance measure and better informed program offices by enhancing communication and training.

Security Control Review of the CFPB’s Active Directory Implementation (nonpublic report)

2017-IT-C-008

April 17, 2017

Total number of recommendations: 1

Recommendations open: 1

See the [summary](#) in the body of this report.

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: 6

See the [summary](#) in the body of this report.

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: 8

See the [summary](#) in the body of this report.

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: 9

See the [summary](#) in the body of this report.

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

See the [summary](#) in the body of this report.

The CFPB Can Improve Its Examination Workpaper Documentation Practices

2017-SR-C-016

September 27, 2017

Total number of recommendations: 17

Recommendations open: 17

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
IRS	Internal Revenue Service
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

PRA	prompt regulatory action
SEFL	Division of Supervision, Enforcement, and Fair Lending
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

