Office of Inspector General

Semiannual Report to the Congress

April 1, 2016 – September 30, 2016

FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

The Federal Deposit Insurance Corporation (FDIC) is an independent agency created by the Congress to maintain stability and confidence in the nation's banking system by insuring deposits, examining and supervising financial institutions, and managing receiverships. Approximately 6,200 individuals carry out the FDIC mission throughout the country. According to most current FDIC data, the FDIC insured more than $6.68 trillion in deposits in 6,058 institutions, of which the FDIC supervised 3,878. As a result of institution failures during the financial crisis, the balance of the Deposit Insurance Fund turned negative during the third quarter of 2009 and hit a low of negative $20.9 billion by the end of that year. The FDIC subsequently adopted a Restoration Plan, and with various assessments imposed over the past few years, along with improved conditions in the industry, the Deposit Insurance Fund balance has steadily increased to a positive $77.9 billion as of June 30, 2016. Receiverships under FDIC control as of August 30, 2016, totaled 403, with about $3.9 billion in assets.

Office of Inspector General

Semiannual Report to the Congress

April 1, 2016 – September 30, 2016

Federal Deposit Insurance Corporation

Acting Inspector General's Statement

I am pleased to present the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) semiannual report for the period April 1, 2016 through September 30, 2016. The work highlighted in this report reflects our commitment to promote economy, efficiency, effectiveness, and integrity in FDIC programs and operations, and to make a positive impact in the banking industry.

During the reporting period, we issued six audit and evaluation reports and made 16 recommendations covering topics such as information security, the Corporation's process for reviewing resolution plans submitted under Section 165(d) of the Dodd-Frank Wall Street Reform and Consumer Protection Act, receivership asset securitization controls, corporate readiness to implement the Digital Accountability and Transparency Act of 2014, and required information under the Cybersecurity Act of 2015. Our investigations of criminal activity affecting the FDIC and the banking industry resulted in 39 indictments; 37 convictions; 17 arrests; and potential fines, restitution, and asset forfeitures totaling nearly $43 million. Many subjects in these investigations were former bank officers and directors who abused their positions of trust and are now paying a high price for their crimes.

We also continued to focus on other key goals—effectively communicating with stakeholders, expanding our knowledge and understanding of emerging risk areas, and ongoing efforts to increase operational efficiency and promote excellence in our workforce. Activities in these areas are more fully explained in this report.

A primary focus over the past 6-month period has been our work involving the FDIC's identification and reporting of information security breaches and the related matter of the FDIC's protection of sensitive information. We believe candid and transparent discussion of our findings is critical as the FDIC, the banking industry, and the government more broadly confronts the array of security threats present in the modern world. We discuss the results of our work on these issues in detail in this semiannual report.

Importantly, our dual reporting responsibility under the IG Act requires that we keep not only the head of the agency but also the Congress fully and currently informed about problems and deficiencies in agency programs and operations, as well as the necessity for and progress of corrective action. In fact, one of the Congress' foremost functions under the Constitution is the power to oversee the Executive branch. In that regard, I was asked to testify on two occasions before the Committee on Science, Space, and Technology, U.S. House of Representatives, during the reporting period. These hearings shed light on the Corporation's information security posture and the manner in which the FDIC has responded to Committee requests for information and document productions.

At the first of these hearings, I testified with the FDIC's Chief Information Officer. At the second hearing, I testified along with the FDIC Chairman. Each hearing is a concrete example of the position an IG often occupies, and the constructive tension intended by the dual reporting arrangement. Our work on these matters is not yet done. Given the critical significance of the risks in the FDIC's information security environment, we continue to conduct follow-on assignments for the Committee as well as new work requested by the Chairman of the Senate Banking Committee to address cybersecurity concerns, and we may be called upon again to testify.

I commend the dedicated members of the OIG who have worked tirelessly over the past 6 months, especially those responsible for bringing awareness to serious information security risks at the FDIC. On behalf of the OIG, I underscore our continuing commitment to our stakeholders—the FDIC, Congress, other regulatory agencies, IG community colleagues, law enforcement partners, and the public. We rely on the continued strength of positive working relationships with each of them as we pursue the IG mission, strive to help the FDIC successfully accomplish its mission, and work in service to the American people.

I would also note, in closing, particularly as we prepare for a new Administration, that the federal government is operating with many IG positions currently vacant, and among those vacancies is the position of FDIC IG. I have been honored to serve as the Acting IG for the past 3 years. Given the significant challenges facing the FDIC and our Nation, my hope is that the Congress will address the FDIC IG vacancy and take steps to provide the FDIC OIG with permanent leadership, in the best interest of our office and the Corporation.

Fred W. Gibson, Jr.
Acting Inspector General
October 2016

Table of Contents

Acronyms and Abbreviations

BDO	BDO USA, LLP
CEO	chief executive officer
CFNB	Citizens First National Bank
CIGFO	Council of Inspectors General on Financial Oversight
CIGIE	Council of the Inspectors General on Integrity and Efficiency
CIO	chief information officer
CY-4	Washington Field Office Cyber Squad-4
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	Department of Justice
DRR	Division of Resolutions and Receiverships
EAR	Equipment Acquisition Resources, Inc.
ECU	Electronic Crimes Unit
FBI	Federal Bureau of Investigation
FDI Act	Federal Deposit Insurance Act
FDIC	Federal Deposit Insurance Corporation
FFATA	Federal Funding Accountability and Transparency Act of 2006
FHFA	Federal Housing Finance Agency
FISMA	Federal Information Security Modernization Act of 2014
FOIA	Freedom of Information Act
FRB	Board of Governors of the Federal Reserve System
FRB-MN	Federal Reserve Bank of Minneapolis

FSOC	Financial Stability Oversight Council
FY	fiscal year
GAO	Government Accountability Office
IG	Inspector General
IRS-CI	Internal Revenue Service Criminal Investigation Division
IT	information technology
MTD	Machine Tools Direct, Inc.
NARA	National Archives and Records Administration
NCIJTF	National Cyber Investigative Joint Task Force
OCC	Office of the Comptroller of the Currency
OCFI	Office of Complex Financial Institutions
OI	Office of Investigations
OIG	Office of Inspector General
OMB	Office of Management and Budget
RAL	refund anticipation loan
RMS	Division of Risk Management Supervision
SAR	Suspicious Activity Report
SBA	Small Business Administration
SIFI	systemically important financial institution
SSGNs	structured sales of guarantee notes
USB	Universal Serial Bus
VFSC	Voyager Financial Services Corporation

Highlights and Outcomes

The FDIC OIG conducts its work in five strategic goal areas that are linked to the OIG's mission. A summary of our completed work during the reporting period, along with references to selected ongoing assignments, is presented below, by goal area. We revised our previous goals as we planned for fiscal year (FY) 2017 and continue to refine performance goals and associated performance measures for the upcoming fiscal year.

Goal 1: Quality Audits and Evaluations

Conduct quality audits, evaluations, and other reviews to ensure economy, efficiency, and effectiveness in FDIC programs and operations

We issued six final audit or evaluation reports during the reporting period. Of note, in one we examined the FDIC's reporting of major information security incidents, as required by the Federal Information Security Modernization Act (FISMA) of 2014 and related Office of Management and Budget (OMB) guidance, and we made five recommendations to the Chief Information Officer (CIO) to provide the FDIC greater assurance that major information security incidents will be reported consistent with FISMA and OMB guidance. We also issued a related report on the FDIC's safeguarding of resolution plans submitted under the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act). This report was prompted by a situation where an FDIC employee abruptly resigned and took sensitive components of resolution plans without authorization. We made a recommendation in that report regarding the Corporation's establishing an insider threat program, an initiative that it had begun but not yet completed and five other recommendations to strengthen information security controls to protect information in the resolution plans. At the end of the reporting period, the FDIC had formally established an insider threat and counterintelligence program. Importantly, these two reports received Congressional, media, and public attention, and the Acting Inspector General (IG) testified on two occasions—first with the FDIC CIO and then with the FDIC Chairman—before the Committee on Science, Space, and Technology, U.S. House of Representatives, as that Committee conducted oversight of the cybersecurity posture of the FDIC.

In the area of resolutions and receiverships, we issued a report on the FDIC's controls over receivership asset securitizations and reported that for the most part, the Corporation had controls in place to sufficiently mitigate risk associated with the receivership asset securitization process. We did find that opportunities existed for the FDIC to better document processes performed in procedures and job aids and to enhance certain controls and we made six recommendations in that regard. We also issued the results of an evaluation of the FDIC's resolution plan review process, where we assessed how the FDIC determines whether resolution plans are informationally incomplete and shortcomings exist to the plans' credibility. We concluded that the review teams complied with the established framework for conducting completeness and shortcomings reviews, and the teams assessed the eight systemically important financial institution (SIFI) resolution plans in our sample in a consistent manner.

We also completed two assignments required of federal OIGs during the reporting period. In the first, we conducted work required by the Digital Accountability and Transparency Act of 2014 (DATA Act), looking at the Corporation's preparedness to implement requirements of the Act. We reported that the FDIC had completed certain recommended steps for implementing the Act, had taken actions to strengthen controls in that regard, and was continuing to address remaining steps as of the end of our fieldwork. Additionally, we undertook a review to describe the FDIC's information security policies, procedures, practices, and capabilities for covered systems under Section 406 of the Cybersecurity Act of 2015—that is, systems that provide access to personally identifiable information. We reported that the FDIC had 269 systems meeting the definition of covered systems and that policies for those systems generally reflected appropriate standards such as those issued by OMB and recommended security controls and practices contained in National Institute of Standards and Technology publications and federal statutes. We did note, however, that although system access controls were in place, recent audits indicated that appropriate standards had not always been followed.

We received an update on the Corporation's responsive actions to an earlier report involving its supervisory approach to refund anticipation loans. Ongoing assignments in support of this goal include reviews of the FDIC's monitoring of SIFIs, shared loss agreement recoveries, technology service provider contracts with FDIC-supervised institutions, the FDIC's Failed Bank Data Services project, and progress the FDIC has made in addressing credentialing and multi-factor authentication issues that we highlighted in an earlier audit. Also of note, the Office of Audits and Evaluations completed its FY 2017 assignment plan during the reporting period, outlining a comprehensive program of reviews to assist the Corporation in carrying out its mission, programs, and operations.

Goal 2: Impactful Investigations

Investigate criminal activities affecting financial institutions and conduct other investigative activities to ensure integrity in the banking industry and FDIC internal operations

Our Office of Investigations (OI) continued its work addressing criminal activity affecting both open and closed financial institutions. A number of cases we highlight in this report were referred to us by the FDIC's Division of Risk Management Supervision (RMS) and the Division of Resolutions and Receiverships (DRR). Cases during the reporting period included those involving former bank directors and officers, employees of the bank, real estate professionals, attorneys, businessmen, and other bank customers. In a case involving an Arkansas bank, for example, three former bank employees who had each been employed by the bank for over 35 years, received lengthy prison sentences and were ordered to pay a total of more than $3.9 million in restitution for stealing that much money from the bank's vault over a 10-year period. In another case, a former vice president of Mechanics Bank in Water Valley, Mississippi, was sentenced to serve 24 months in prison and ordered to pay $3.3 million in restitution following his guilty plea to bank fraud. He misused his position and manipulated bank account records to make unauthorized extensions of credit for the benefit of certain bank customers, concealed his activity from the bank's officers and board of directors, and embezzled funds for his personal benefit. Another case involved the sentencing of two individuals who had engaged in criminal activity at La Jolla Bank, La Jolla, California. One was a broker sentenced for lying to investigators and obstructing a bribery investigation. The other was a bank manager who was sentenced for conspiracy to misapply bank funds while managing the Small Business Administration lending department of the bank.

OI special agents continued to partner with U.S. Attorneys' Offices throughout the country and participated actively in working groups with law enforcement partners to leverage knowledge and better address issues of mutual concern. Our special agents also offered training in fraud detection, and engaged in outreach with groups both internal and external to the FDIC to explain OI's role in combatting criminal activity causing harm to the banking system. Overall investigative results for the reporting period attest to the value of solid working relationships with the Corporation, other OIGs, and law enforcement partners. Our investigations during the past 6 months led to 39 indictments; 37 convictions; 17 arrests; and potential fines, restitution, and asset forfeitures totaling nearly $43 million.

Goal 3: Effective Communications

Communicate effectively with internal and external stakeholders

In support of this goal, we continue to reexamine the information needs of the OIG's stakeholders, including the FDIC Board of Directors and FDIC division and office management and their staffs, the Congress, members of the IG community, the Government Accountability Office (GAO), OMB, the media, and the general public. We do so in the interest of ensuring that our communications are effective and that the messages we convey are transparent, informative, and clearly understood.

We place a high priority on maintaining positive working relationships with the FDIC Chairman, Vice Chairman, other FDIC Board members, and management officials. During the reporting period, the Acting IG and other OIG senior executives met regularly with the Chairman, Vice Chairman, and other senior officials; attended FDIC Board meetings; and presented the results of completed work at FDIC Audit Committee meetings.

We also maintained positive relationships with the Congress and provided timely responses to a number of congressional inquiries. Congressional interaction during the reporting period included updates to the House Financial Services Committee regarding our work related to the FDIC's supervisory approach to refund anticipation loans; the Acting IG's testimonies before the Committee on Science, Space, and Technology, U.S. House of Representatives, related to our reports on the FDIC's reporting of major information security incidents and the FDIC's controls for mitigating the risk of an unauthorized release of sensitive resolution plans submitted under Section 165(d) of the Dodd-Frank Act; follow-on issues related to those testimonies, including a request on the part of the Senate Banking Committee that our office further review the FDIC's reporting of major information security incidents; and information on the status of open, unimplemented recommendations; closed audits, evaluations, and investigations that were not made available to the public; and referrals to the Department of Justice (DOJ) and associated criminal prosecutions.

The OIG fully supported and participated in IG community activities through the Council of the Inspectors General on Integrity and Efficiency (CIGIE). We coordinated with representatives from the other financial regulatory OIGs and others in the IG community on issues of mutual interest. We assisted in several CIGIE training initiatives and participated in the Federal Audit Executive Council's DATA Act Working Group. Also, in this regard, the Dodd-Frank Act created the Financial Stability Oversight Council (FSOC) and further established the Council of Inspectors General on Financial Oversight (CIGFO). This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. We attended CIGFO meetings and participated on a CIGFO working group to evaluate FSOC's efforts to promote market discipline.

We continue to field allegations through our Hotline system and receive inquiries on varied topics from the public through other means, and we make every effort to respond timely to such contacts. During the reporting period, several of the Hotline allegations we received warranted further review, and our Office of Audits and Evaluations is pursuing those, with reports expected during the upcoming semiannual period. We are in the process of updating and refining our Congressional protocols and also developing a more formal and effective means of handling media requests and inquiries. Ongoing efforts to redesign our external Website are intended to provide more useful content and better serve all stakeholders.

In the interest of informing the new Administration and new Congress of the FDIC OIG's role, mission, and contributions to good government, we have produced transition materials related to our office for dissemination after the November 2016 elections.

Goal 4: Enhanced Understanding of Emerging Issues
Continuously seek to enhance OIG knowledge and understanding of emerging and evolving issues affecting the FDIC, OIG, and insured depository institutions

Our attention to better understanding of emerging issues continued to focus on two matters in particular during the reporting period. First, we continued to expand our involvement and knowledge of cyber security matters in several ways. One of our senior managers serves as a cybersecurity liaison officer to proactively monitor cyber issues and trends from multiple sources and disseminate pertinent information to interested or affected parties both internal and external to the FDIC. He monitors activities of the Corporation's Data Breach Management Team and is a member of the Corporation's Insider Threat and Counterintelligence Program working group. Our information security manager, information technology (IT) professionals in the Office of Audits and Evaluations, members of the OIG's Electronic Crimes Unit, and a Special Advisor to the Acting IG play key roles in the cybersecurity arena. Working together, these resources keep current on possible threats to ensure our readiness to address them. We also continued our active participation at the Federal Bureau of Investigation's (FBI) Cyber Task Force in Washington, D.C. and continue to devote an investigative resource to the National Cyber Investigative Joint Task Force. We participated in training activities sponsored by the First Information Operations Command of the U.S. Army related to defense and intelligence roles in addressing cyber threats. These efforts are paying dividends in terms of increased knowledge and productive networking and information-sharing opportunities. Additionally, ongoing audit and evaluation assignments are addressing significant information security topics and those efforts further expand our knowledge base.

A second priority area of focus for our office is on the implications of the Dodd-Frank Act, and in particular, on the responsibilities that our office would be required to fulfill were a SIFI to fail. These responsibilities would include analyses and reporting on various aspects of the FDIC's liquidation of any covered financial company by the Corporation as receiver under Title II of the Act. We researched the impact of such responsibilities and identified issues relating to scope, frequency, reporting, funding, and coordination efforts that would be needed to successfully meet the mandate of the Dodd-Frank Act. We are continuing to pursue those issues.

Goal 5: Operational Efficiency and Workforce Excellence
Maximize OIG operational efficiency and workforce excellence

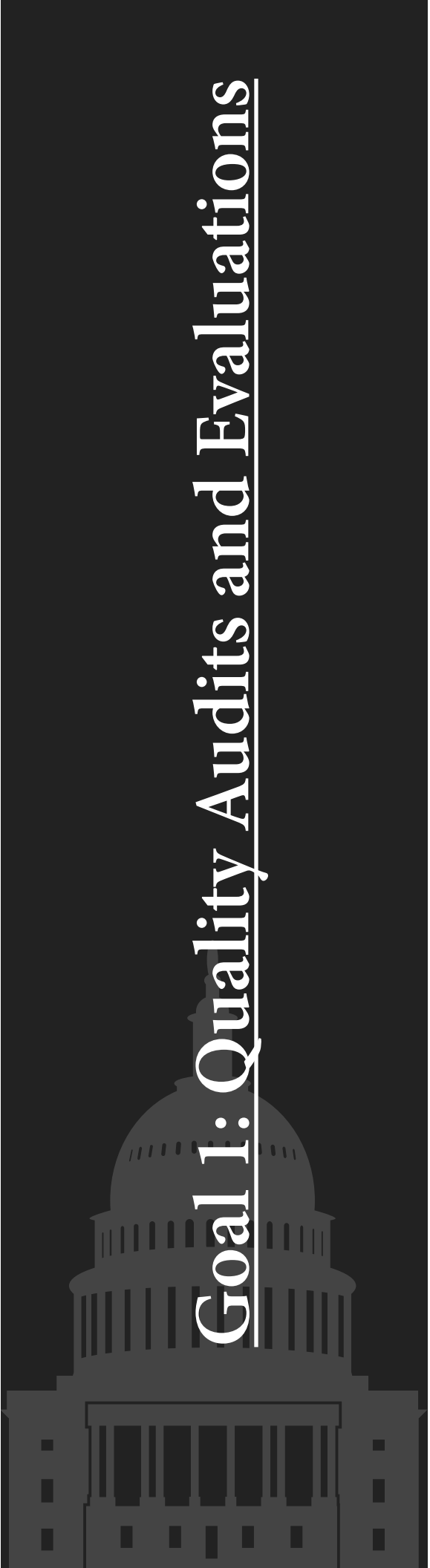
We have devoted ongoing attention to enhancing operational efficiencies and workforce excellence. With an emphasis on our human resources and the talents needed for OIG success, we carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. To that end, we formulated our FY 2018 budget request and received the FDIC Chairman's approval of that request for $39.1 million to fund 144 authorized positions, up 7 from FY 2016. We filled several key positions during the reporting period—a Deputy Assistant Inspector General for Investigations, a Special Agent in Charge of the New York Region, a Special Advisor to the Acting IG, to name a few, and planned for upcoming workforce needs by hiring several new financial analysts and audit and evaluation professionals, including those with IT expertise. We also continued to support members of the OIG pursuing professional training and certifications or attending graduate banking school programs to enhance the OIG staff members' expertise and knowledge and enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities. Finally, OIG senior management analyzed the OIG's performance management program and the OIG's process for recognizing and rewarding staff in the interest of providing constructive feedback and acknowledging the efforts of all staff in a fair, transparent, and consistent manner.

During the reporting period, we implemented a new investigative case management system and continued to better track audit and evaluation assignment milestones and costs and to manage audit and evaluation records located in TeamMate or other electronic repositories. In a related vein, we continued efforts to update the OIG's records and information management program and practices to ensure an efficient, effective, and secure means of collecting, storing, and retrieving needed information and documents. We became aware of a situation where OIG to OIG emails were residing in the FDIC's email vault. Given independence concerns with this situation, we took steps to address the problem with the Corporation. We also engaged a contractor to independently examine how the comingling occurred and ensure effective remediation efforts. We took additional steps to maintain a secure, effective, and reliable IT environment and educate OIG staff so that we can leverage the tools we use to conduct our work more efficiently.

We undertook risk-based OIG planning efforts for audits, evaluations, and—to the extent possible—investigations for FY 2017 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. We incorporated such information in broader discussions in finalizing the OIG's comprehensive strategic and performance plans for FY 2017-2021 and FY 2017, respectively.

Significant Outcomes (April 1, 2016 – September 30, 2016)	
Audit and Evaluation Reports Issued	6
Questioned Costs or Funds Put to Better Use	$55,000
Nonmonetary Recommendations	16
Investigations Opened	46
Investigations Closed	34
OIG Subpoenas Issued	14
Judicial Actions:	
Indictments/Informations	39
Convictions	37
Arrests	17
OIG Investigations Resulted in:	
Fines of	$29,321
Restitution of	42,188,200
Asset Forfeitures of	735,758
Total	$42,953,279
Cases Referred to the Department of Justice (U.S. Attorney)	33
Proposed Regulations and Legislation Reviewed	9
Responses to Requests Under the Freedom of Information/Privacy Act	13

Goal 1: Quality Audits and Evaluations



Conduct quality audits, evaluations, and other reviews to ensure economy, efficiency, and effectiveness in FDIC programs and operations

The OIG's work in support of this goal is largely the responsibility of the OIG's Office of Audits and Evaluations. The OIG's Office of Audits provides the FDIC with professional audit and related services covering the full range of its statutory and regulatory responsibility, including major programs and activities. These audits are designed to promote economy, efficiency, and effectiveness and to prevent fraud, waste, and abuse in corporate programs and operations. This office ensures the compliance of all OIG audit work with applicable audit standards, including those established by the Comptroller General of the United States. It may also conduct external peer reviews of other OIG offices, according to the cycle established by CIGIE.

The companion Office of Evaluations evaluates, reviews, studies, or analyzes FDIC programs and activities to provide independent, objective information to facilitate FDIC management decision-making and improve operations. Evaluation projects are conducted in accordance with the *Quality Standards for Inspection and Evaluation*. Evaluation projects are generally limited in scope and may be requested by the FDIC Board of Directors, FDIC management, or the Congress.

Prior to passage of the Dodd-Frank Act, in the event of an insured depository institution failure, the Federal Deposit Insurance Act (FDI Act) required the appropriate regulatory OIG to perform a review when the Deposit Insurance Fund (DIF) incurs a material loss. Under the FDI Act, a loss was considered material to the insurance fund if it exceeded $25 million or 2 percent of the failed institution's total assets. With passage of the Dodd-Frank Act, the loss threshold was increased to $200 million through December 31, 2011, $150 million for losses that occurred for the period January 1, 2012 through December 31, 2013, and $50 million thereafter. The FDIC OIG performs the review if the FDIC is the primary regulator of the institution. The Department of the Treasury OIG and the OIG at the Board of Governors of the Federal Reserve System (FRB) perform reviews when their agencies are the primary regulators. These reviews identify what caused the material loss and evaluate the supervision of the federal regulatory agency, including compliance with the Prompt Corrective Action requirements of the FDI Act.

Importantly, under the Dodd-Frank Act, the OIG is now required to review all losses incurred by the DIF under the thresholds to determine (a) the grounds identified by the state or federal banking agency for appointing the Corporation as receiver and (b) whether any unusual circumstances exist that might warrant an in-depth review of the loss. Although the number of failures continues to decline, we conduct and report on material loss reviews and in-depth reviews of failed FDIC-supervised institutions, as warranted, and continue to review all failures of FDIC-supervised institutions for any unusual circumstances.

During the reporting period, the Office of Audits and Evaluations finalized its *Assignment Plan for FY 2017*. The selected assignments take into account results of the OIG's strategic planning process, which included establishing an inventory of all FDIC programs and activities, evaluating the significance and risk of those programs and activities, and considering management and Congressional interest and statutorily-required reviews. The OIG will seek to ensure that audits and evaluations are relevant, timely, and assist the Corporation in efficiently and effectively carrying out its mission, programs, and operations. The plan also describes various operational and quality assurance initiatives aimed at improving the consistency and efficiency of our processes and quality of our products; recruiting, developing, and engaging staff; leveraging technology more fully in our audits and evaluations; and preparing to address OIG reporting requirements under the Dodd-Frank Act. Of particular importance in the coming year will be completion of a multi-year IT coverage framework to help guide our work in this area and ensure systematic, risk-based audits and evaluations of key operations and activities.

OIG Work in Support of Goal 1

In support of this goal during the reporting period, we issued six reports. These reports contain 16 recommendations, identify questioned cost of $55,000, and span various FDIC programs and activities, including the reporting of major information security incidents, the Corporation's protection of sensitive information in resolution plans submitted under Section 165(d) of the Dodd-Frank Act, its review process of those resolution plans for completeness and shortcomings to their credibility, receivership asset securitization controls, DATA Act readiness, and required information under the Cybersecurity Act of 2015. Our office also continued the legislatively mandated review of all failed FDIC-supervised institutions causing losses to the DIF of less than the threshold outlined in the Dodd-Frank Act to determine whether circumstances surrounding the failures would warrant further review. Our failed bank review activity is presented in Appendix 2.

At the end of the reporting period, ongoing audit and evaluation assignments were addressing such issues as the FDIC's efforts to ensure shared loss agreement recoveries are identified and remitted, technology service provider contracts with FDIC-supervised institutions, controls over separating employees' access to sensitive information, the FDIC's Failed Bank Data Services project, monitoring of SIFIs, and progress made in addressing credentialing and multi-factor authentication activities. Results of these ongoing assignments will be presented in an upcoming semiannual report.

The results of issued audit and evaluation reports are discussed below. Following the discussion of this work, we present an update on a report of inquiry that we issued in March 2016 regarding the FDIC's supervisory approach to refund anticipation loans.

The FDIC's Process for Identifying and Reporting Major Information Security Incidents

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program that includes (among other things) procedures for detecting, reporting, and responding to information security incidents. Such procedures are to include notifying and consulting with, as appropriate, the Congressional Committees referenced in the statute for major incidents. According to FISMA, Congressional notification and consulting is to occur not later than 7 days after the date on which there is a reasonable basis to conclude that a major incident has occurred.

FISMA requires OMB to develop guidance on what constitutes a major incident and directs agencies to report incidents designated as major. Accordingly, OMB issued Memorandum M-16-03, *Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management Requirements*, dated October 30, 2015, (OMB Memorandum M-16-03) that provides agencies with a definition of the term "major incident" and a framework of factors, the combination of which agencies must consider when characterizing an incident as major. The OMB memorandum states that agencies should notify affected individuals, in accordance with FISMA, as "expeditiously as practical, without unreasonable delay." The memorandum adds that although agencies may consult with the Department of Homeland Security's United States Computer Emergency Readiness Team when determining whether an incident is considered a "major incident," it is ultimately the responsibility of the victim agency to make the determination.

We conducted an audit to determine whether the FDIC had established key controls that provide reasonable assurance that major incidents are identified and reported in a timely manner. As part of the audit, we conducted a detailed review of the FDIC's incident investigation-related activities, records, decisions, and reports for one specific incident (referred to in our report as the Florida Incident).

Information security incidents at the FDIC can be identified through a variety of sources. For example, employees and contractors must contact the FDIC's Help Desk/Computer Security Incident Response Team to report a suspected security incident; technologies used by the FDIC to monitor network activity, such as the Data Loss Prevention tool, may identify apparent security policy violations; and outside organizations may notify the FDIC of illegal or suspicious activity involving the FDIC's IT resources.

The FDIC's Information Security and Privacy Staff within the CIO Organization has overall responsibility for analyzing, reporting, and remediating information security incidents. Information Security and Privacy Staff report to the Acting Chief Information Security Officer, who reports to the CIO. The CIO reports to the FDIC Chairman. Other organizational components also play a role in addressing information security incidents. Most notably, the FDIC's Help Desk/Computer Security Incident Response Team provides technical assistance and investigates, reports, resolves, and closes incidents by working with FDIC system administrators, division and office Information Security Managers, Privacy Program Office staff, the Data Breach Management Team for data breaches, and others.

Our audit focused on the FDIC's processes for addressing one particular type of information security incident—a breach of sensitive information—because the incident we selected for detailed review (i.e., the Florida Incident) was a breach. The Florida Incident involved a former FDIC employee who copied a large quantity of sensitive FDIC information, including personally identifiable information, to removable media and took this information when the employee departed the FDIC's employment in October 2015. The FDIC detected the incident through its Data Loss Prevention tool.

We reported that although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents were identified and reported in a timely manner. Specifically, we found that:

- The FDIC's incident response policies, procedures, and guidelines did not address major incidents.
- The large volume of potential security violations identified by the Data Loss Prevention tool, together with limited resources devoted to reviewing these potential violations, hindered meaningful analysis of the information and the FDIC's ability to identify all security incidents, including major incidents.

Further, based on our analysis of the Florida Incident, we concluded that the FDIC had not properly applied the criteria in OMB Memorandum M-16-03 when it determined that the incident was not major. Specifically, the FDIC based its determination on various mitigation factors related to the "risk of harm" posed by the incident. Although such factors have relevance in determining the mitigation actions to be taken in addressing incidents, the factors are not among those listed in OMB Memorandum M-16-03 for agencies to consider when determining whether incidents are major and, therefore, are not relevant. We notified the CIO on February 19, 2016 that our analysis of the Florida Incident found that reasonable grounds existed to designate the incident as major as of December 2, 2015, and, as such, the incident warranted immediate reporting to the Congress. The FDIC subsequently reported the Florida Incident to the Congress as major on February 26, 2016.

When the FDIC did notify the Congress of the incident, certain risk mitigation factors in the notifications were either unsupported by adequate evidence and/or inconsistent with information available at the time. As a result, in our view, the notifications did not accurately portray the extent of risk associated with the incident. Our analysis of the Florida Incident also found that:

- More than 4 weeks had elapsed between the initial discovery of the incident and a determination that the incident was a breach.
- The decision about whether individuals and organizations potentially affected by the incident would be notified was untimely, and a required notification to another federal agency was not made in a timely manner.
- Records documenting investigative activities were not centrally managed and sometimes contained unreliable information, and the underlying rationale and discussions pertaining to certain decisions were not always documented.

The results of our analysis of the Florida Incident prompted the CIO to initiate a review of similarly situated information security incidents that occurred after the OMB issued Memorandum M-16-03 to determine whether additional incidents warranted designation as major. The CIO's review resulted in six additional incidents being reported to the Congress as major between March and May 2016.

On May 5, 2016, the CIO provided our office with an outline of a plan describing a number of initiatives aimed at addressing policy and program shortcomings in the FDIC's incident response processes. Such initiatives include, but are not limited to, developing an overarching incident response program guide, hiring an incident response coordinator, implementing a new incident tracking system, updating incident response policies and procedures, and performing a comprehensive assessment of the FDIC's information security and privacy programs.

We made five recommendations to the CIO that were intended to provide the FDIC with greater assurance that major incidents will be identified and reported consistent with FISMA and OMB Memorandum M-16-03. We noted that addressing these recommendations would facilitate the Congress' ability to provide the oversight intended by FISMA and contribute to the OMB's goal of having effective interagency communication so that incidents are mitigated appropriately and as quickly as possible. FDIC management concurred with the recommendations and described planned actions that were responsive.

The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans

Section 165(d) of the Dodd-Frank Act requires certain financial companies designated as systemically important to report to the FDIC on their plans for a rapid and orderly resolution under the Bankruptcy Code in the event of material financial distress or failure. To implement the requirements of section 165(d), the FDIC and the FRB jointly issued a Final Rule, entitled *Resolution Plans Required*, dated November 1, 2011. The Final Rule requires financial companies covered by the statute to submit resolution plans, sometimes referred to as "living wills," to the FDIC and FRB for review. The resolution plans required by the Dodd-Frank Act contain some of the most sensitive information that the FDIC maintains. Accordingly, safeguarding the plans from unauthorized access or disclosure is critically important to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system.

In September 2015, an employee working in the FDIC's Office of Complex Financial Institutions (OCFI) abruptly resigned from the Corporation and took sensitive components of resolution plans without authorization. We conducted an audit to determine the factors that contributed to this security incident involving sensitive resolution plans and assess the adequacy of mitigating controls established subsequent to the incident.

By way of background, on September 29, 2015, FDIC personnel detected that an employee who had previously worked for OCFI had copied sensitive components of three resolution plans from the network onto an unencrypted Universal Serial Bus (USB) storage device. This activity violated OCFI policy which expressly prohibits the storage of resolution plans on removable media. In addition, the activity appeared suspicious because the information was copied to the USB device immediately prior to the employee's departure. Further, the employee did not have authorization to take any sensitive FDIC information, including resolution plans, upon departure.

Law enforcement officials subsequently recovered the USB device that contained the components of the resolution plans copied by the employee. In the course of doing so, these officials also identified and recovered from the employee a sensitive Executive Summary for a fourth resolution plan that was in hard copy. In early October 2015, OCFI officials coordinated with RMS to notify each of the SIFIs impacted by the incident. In addition, law enforcement officials learned that the employee had interviewed for employment with two of the four SIFIs impacted by the incident following the employee's resignation, suggesting that the employee may have taken the resolution plans for personal gain. Further, there were indications prior to the incident that the employee presented a heightened security risk and may not have been suited to have access to highly sensitive information, such as resolution plans.

The incident involving resolution plans is not an isolated instance of unauthorized exfiltration of sensitive FDIC information by trusted insiders leaving the Corporation. As discussed earlier in this semiannual report, between February and May 2016, the FDIC notified the Congress of seven major incidents in which employees took significant quantities of sensitive information from the FDIC without authorization when they departed. Individuals that organizations entrust with access to sensitive information pose specific types of security risks to organizations. Accordingly, special consideration must be given to the risks posed by trusted insiders and appropriate security controls established to mitigate those risks.

We identified a number of factors that contributed to the security incident involving sensitive resolution plans. Most importantly, our report noted that an insider threat program would have better enabled the FDIC to deter, detect, and mitigate the risks posed by the employee. In addition, a key security control designed to prevent employees with access to sensitive resolution plans from copying electronic information to removable media failed to operate as intended. The remaining factors involved OCFI employees having access to resolution plans that exceeded business needs; OCFI's inability to effectively review and revoke employee access to resolution plans because employees were allowed to store copies of the plans outside of the FDIC's official system of record—OCFI Documentum; and OCFI's inability to monitor all downloading of resolution plans stored in OCFI Documentum.

With respect to insider threats, the FDIC has a number of long-standing controls designed to mitigate risks associated with trusted insiders. Such controls include, for example, background investigations, periodic inspections of FDIC facilities to identify security concerns, employee non-disclosure agreements, a Data Loss Prevention tool, and programs to help employees cope with personal issues. During 2014 and 2015, the FDIC began to take steps toward establishing a formal insider threat program by, among other things, developing a proposed governance structure and drafting program policies. However, these activities were not completed or approved, and progress toward establishing an insider threat program stalled in the fall of 2015.

Following the incident involving resolution plans, OCFI officials assessed the associated risks and began implementing new or enhanced security controls over resolution plans. Such controls included better aligning employee access to resolution plans in OCFI Documentum with business needs; increasing the frequency of access reviews for plans stored in OCFI Documentum; and reviewing employee printing activities to identify and investigate suspicious activity. However, because OCFI had not yet developed written policies, procedures, and assessment plans to govern these new or enhanced controls, we did not have criteria against which to test their effectiveness.

Our report describes additional control improvements that the FDIC should implement to better safeguard sensitive resolution plans. It is important to note that no matter how well designed, implemented, or operated, an internal control system cannot provide absolute assurance that all of management's objectives will be met. Factors outside of management's control, such as a trusted insider who is intent on circumventing internal controls, can affect management's ability to achieve its objectives. Accordingly, the control measures we are recommending are intended to help the FDIC achieve reasonable, not absolute, assurance that sensitive resolution plans are adequately safeguarded.

We made six recommendations in the report. One recommendation was addressed to the Deputy to the Chairman, Chief Operating Officer, and Chief of Staff to work with other senior FDIC executives to establish a corporate-wide insider threat program. The remaining five recommendations dealt with strengthening the FDIC's information security controls, particularly with respect to safeguarding sensitive resolution plans submitted to the Corporation under the Dodd-Frank Act. FDIC management concurred with the recommendations.

Testifying Before Congress

During the reporting period, the Acting Inspector General was called upon to testify on two occasions before the Committee on Science, Space, and Technology, U.S. House of Representatives regarding the OIG's recent and continuing work related to cybersecurity and protection of sensitive information at the FDIC. During the first hearing on May 12, 2016, the Acting IG was not as free to speak to the issues that were unfolding, as the work was ongoing and not yet public. By mid-July, however, the OIG had issued two reports on these matters—one related to reporting major security incidents and the other on protecting sensitive resolution plans—and the Acting IG was able to provide additional information and to respond more fully to Committee Members' questions. The Acting Inspector General testified along with the FDIC's Chief Information Officer at the May hearing and subsequently with the FDIC Chairman at the July 14 hearing. Links to the testimonies are located at www.fdicig.gov. We continue efforts on new assignments to address certain issues raised at and after the hearings and may be called to testify again as that new work is finalized.

Update: Following the issuance of our preliminary results on the audit in May 2016, senior FDIC management placed a high priority on establishing a formal insider threat program. Specifically, the Executive Management Committee began meeting with responsible division and office managers on a weekly basis and an independent consultant was engaged to advise the FDIC on how the program should be tailored to meet the FDIC's needs. On September 20, 2016, the Insider Threat and Counterintelligence Program was formally established.

The FDIC's Controls Over Receivership Asset Securitizations

As receiver for failed financial institutions, the FDIC uses securitizations and structured sales of guarantee notes (SSGNs) to dispose of certain performing and non-performing residential mortgage loans, commercial loans, construction loans, and mortgage-backed securities held by receiverships. Monthly loan payments of principal and interest are collected from the underlying loans and mortgage-backed securities, and these payments are distributed to the note holders, which includes FDIC receiverships. As of March 31, 2016, there were seven whole loan securitizations and five SSGNs with a total collateral value of $3.2 billion.

The FDIC, in its corporate capacity, guarantees the timely payment of principal and interest due on most of the senior notes in exchange for a fee (guarantee fee). As of December 31, 2015, the FDIC collected guarantee fees totaling approximately $265 million, of which $142 million was from SSGNs and securitization guarantee fees and $123 million was from limited liability company guarantee fees, and recorded a receivable for additional guarantee fees of approximately $26 million.

We contracted with BDO USA, LLP (BDO) to evaluate select key controls over the FDIC's receivership asset securitizations, following their origination, to ensure those controls are performing as intended. BDO focused on DRR processes and controls associated with monitoring receivership asset securitizations and the information DRR provides to the Division of Finance for receivership asset securitization accounting.

BDO did not discover any significant deficiencies in DRR processes and controls associated with monitoring receivership asset securitizations and SSGNs following their originations. BDO's testing found that, for the most part, DRR has controls in place to sufficiently mitigate risk associated with the receivership asset securitization program. DRR has established an organizational structure, delegated authority, and assigned responsibility for carrying out program objectives. DRR has also developed procedures and job aids for monitoring securitizations and SSGNs and channels for communicating program information within and between divisions. In particular, the semiannual valuation of the Asset Loss Reserve involves a multistep review and approval process that involves multiple personnel within and external to DRR.

BDO concluded, however, that opportunities exist for DRR to better document processes performed in procedures and job aids and to enhance certain controls. BDO also observed key personnel dependencies within DRR's Capital Markets Group and closing and post-closing contractors with whom FDIC staff work that could present segregation of duties and knowledge management risks should these individuals leave the Corporation in the future. Finally, BDO identified an overpayment totaling $55,000, which appeared to be an isolated incident and not a control weakness warranting a recommendation. DRR is working to recover this questioned amount from the custodian.

The report contains six recommendations addressed to the Director, DRR, to address the issues we identified. The Director, DRR, concurred with BDO's recommendations.

The FDIC's Resolution Plan Review Process

As referenced earlier, section 165(d) of the Dodd-Frank Act requires bank holding companies with $50 billion or more in consolidated assets and nonbank financial companies designated by FSOC to periodically submit to the FDIC, the Federal Reserve Board, and FSOC, resolution plans that detail how the companies could be resolved in a rapid and orderly manner in the event of material financial distress or failure. The FDIC and Federal Reserve Board then determine whether the plans are complete and credible for achieving that purpose.

The FDIC and the Federal Reserve Board may jointly determine that a plan is not credible or would not facilitate an orderly resolution of the company under the Bankruptcy Code as part of their new authorities. If a company ultimately fails to submit a plan that demonstrates its resolvability in bankruptcy, the FDIC and the FRB may jointly impose more stringent capital, leverage, or liquidity requirements on the company or its subsidiaries. Additionally, the agencies may restrict a firm's growth, activities, or operations.

During the reporting period, we assessed the FDIC resolution plan review process for determining whether (1) resolution plans are informationally incomplete and (2) shortcomings exist to the plans' credibility. The FDIC Board of Directors uses information resulting from the resolution plan review process when determining whether the resolution plans are not credible. We judgmentally selected 8 of the 12 resolution plans submitted as of July 1, 2015, and evaluated the resolution plan review process conducted from July 2015 to September 2015.

We reported that the FDIC established a process and framework for determining whether resolution plans are informationally incomplete and identifying any shortcomings to the plans' credibility. The FDIC also built controls within the process to promote consistency and help ensure that management's program objectives are met. For example, the FDIC provided guidance to the resolution plan reviewers for conducting the completeness and shortcomings assessments. Program controls also included assigning qualified reviewers who had experience with large bank analysis and/or resolution plan reviews; developing relevant training and standardized templates for conducting the plan reviews and documenting the results; and building multiple levels of review and supervision into the review process, including an executive oversight group function.

Based on our review of eight resolution plans, the plan review teams complied with the established framework for conducting completeness and shortcomings reviews, and we concluded the review teams assessed the eight SIFI resolution plans in a consistent manner. In addition, the FDIC met its Dodd-Frank Act requirement for reviewing and notifying the firms of their plans' informational completeness within 60 days of receipt.

During the course of our evaluation, resolution plan review team members provided suggestions for enhancing the resolution plan review process. We communicated these suggestions to senior OCFI and RMS-CFI officials for their consideration at the conclusion of our fieldwork.

It is important to note that our evaluation addressed the FDIC's program and process for assessing the resolution plans. We did not perform work to evaluate the FDIC's conclusions based on the resolution plan reviews or the effectiveness of the firms' plans in resolving a SIFI failure or mitigating financial system disruption.

The Directors of OCFI and RMS concurred with the report's conclusions.

The FDIC's Preparedness Efforts to Implement the Requirements of the DATA Act

The DATA Act expanded the Federal Funding Accountability and Transparency Act of 2006 (FFATA) to increase accountability and transparency in federal spending, and for other purposes. Under the DATA Act, federal IGs are required to (1) review a statistically valid sample of spending data submitted by their agency pursuant to the statute and (2) report on the completeness, timeliness, quality, and accuracy of the data as well as the implementation and use of government-wide data standards. A total of three IG reports are required by the statute: the first is due in November 2016, and the remaining two are due in November 2018 and November 2020.

A timing anomaly exists, however, with respect to the IG reports. Specifically, agencies are not required to report financial and payment information in accordance with the data standards established under the DATA Act until May 2017. As a result, IGs cannot report on the spending data submitted under the Act by November 2016, as the data will not exist until the following year. Thus, as an interim measure, CIGIE encouraged IGs to conduct readiness reviews of their agencies' efforts to address the requirements of the DATA Act in advance of the first required report in November 2017. We conducted such an audit during the reporting period.

The DATA Act required OMB and the Treasury to jointly develop government-wide data standards that include common data elements for reporting financial and payment information and to issue guidance to federal agencies to assist in carrying out their DATA Act reporting requirements. Subsequent to the enactment of the statute, OMB and the Treasury identified 57 data elements that required standardized definitions, consisting of 8 new data elements required by the DATA Act and 49 existing data elements from FFATA. In addition, OMB issued various memoranda containing guidance and the Treasury published the DATA Act Implementation Playbook (the Playbook) containing eight recommended steps that agencies can take as they develop their methodology for DATA Act implementation.

The FDIC's Legal Division determined that although FFATA applies to the FDIC, only federal awards involving the use of funds obtained through the appropriations process are intended to be subject to that Act's reporting requirements. Because the FDIC is not subject to an annual appropriation, the Legal Division concluded that the Corporation is not subject to the reporting requirements of FFATA. The Legal Division also determined that the FDIC is subject to the reporting requirements of the DATA Act. Therefore, the FDIC plans to report on the 8 data elements added by the DATA Act, but not the 49 existing data elements from FFATA that OMB determined required standardization.

We reported that the FDIC has completed the first four steps recommended in the Playbook for implementing the requirements of the DATA Act. Specifically, the FDIC:

- established a DATA Act team comprised of subject matter experts and appointed a senior accountable official who has overall responsibility for implementing the DATA Act.
- reviewed the standardized data elements and determined which data elements the FDIC must report.
- created a data inventory and identified associated business processes, determined the source systems to extract needed data, and identified potential gaps.
- developed a plan to address minimal required changes to systems and business processes and submitted to OMB, and effectively carried out, an implementation plan.

Further, in response to our informal feedback during the audit, the Division of Finance took actions to strengthen controls over the FDIC's preparedness efforts to implement the requirements of the DATA Act. Such actions included, for example, documenting the roles and responsibilities for each DATA Act team member, recording key decisions and actions from team meetings, and formalizing the review and approval of deliverables submitted to OMB and the Treasury.

With respect to the remaining four steps in the Playbook, we noted that the FDIC developed a project plan and initiated various activities, such as: (1) updating the mapping of agency data to the DATA Act schema; (2) implementing information system changes and extracting data; (3) testing Broker outputs to ensure data were complete, accurate, and reliable (A Broker is an intermediary system used to standardize data formatting and assist agencies in validating their data submissions before the data are submitted to the Treasury.); and (4) establishing a schedule to process data submissions. The DATA Act team was continuing to address the remaining Playbook steps at the close of our fieldwork.

We did not make recommendations in our report. Consistent with our oversight responsibilities under the DATA Act, we will continue to review and report on the FDIC's efforts to implement the requirements of the DATA Act in the coming years. We will also continue to monitor the unresolved issue involving agency responsibilities for reporting awards funded through a non-annual appropriations process, and its potential impact on the FDIC's reporting requirements.

The Cybersecurity Act of 2015—The FDIC's Controls and Practices Related to Covered Systems

On December 18, 2015, the President signed the Cybersecurity Act of 2015 into law. Among other things, the statute requires the IG of each federal agency that operates a national security system or a computer system that provides access to personally identifiable information—collectively referred to as "covered systems"—to submit a report to the appropriate committees of jurisdiction in the United States Senate and the House of Representatives. In general, the report is to contain information collected from the agency on various computer security-related topics pertaining to covered systems.

We engaged the professional services firm of Cotton & Company LLP to conduct an audit to describe the FDIC's information security policies, procedures, practices, and capabilities for covered systems as prescribed by Section 406 of the Act. Consistent with the provisions of the statute, the audit generally did not include an assessment of the adequacy of the FDIC's information security controls over covered systems.

Section 406, *Federal Computer Security*, states that the report submitted by the Inspector General shall include a description of the:

- logical access policies and practices used by the agency to access a covered system, including whether appropriate standards were followed;
- logical access controls and multi-factor authentication used by the agency to govern access to covered systems by privileged users, and if such measures are not being used, the reasons why;
- policies and procedures followed to conduct inventories of the software present on covered systems and the licenses associated with such software;
- capabilities utilized by the agency to monitor and detect exfiltration and other threats, including data loss prevention, forensics and visibility, or digital rights management (including, if applicable, the reasons for not using the three referenced capabilities); and
- policies and procedures with respect to ensuring that entities, including contractors, that provide services to the agency are implementing certain information security management practices described above.

We reported that as of May 2016, the FDIC had 269 information systems that met the definition of a covered system and we described the FDIC's information security policies, procedures, practices, and capabilities for these systems.

With respect to logical access to covered systems, our report noted that the policies Cotton & Company LLP reviewed generally reflected appropriate standards, such as government-wide policy and guidance issued by OMB, recommended security controls and practices contained in the National Institute of Standards and Technology's Special Publications, and requirements contained in federal statutes, such as the Privacy Act of 1974 and FISMA. The report also noted, however, that recent audits of the FDIC's information security controls and practices, some of which pertain to covered systems, found that although the FDIC generally had system access controls in place, appropriate standards had not always been followed as evidenced by the findings and recommended control improvements identified during the audits. Consistent with this audit's objective, our report did not contain recommendations.

Update on OIG Report of Inquiry: FDIC's Supervisory Approach to Refund Anticipation Loans and the Involvement of FDIC Leadership and Personnel

In our previous semiannual report, we reported on our work involving the Corporation's supervisory approach to financial institutions that offered a credit product known as a refund anticipation loan (RAL). A RAL is a particular type of loan product, typically offered through a national or local tax preparation company in conjunction with the filing of a taxpayer's income tax return. The tax preparer, often referred to as an electronic refund originator, works in cooperation with the financial institution to advance a portion of the tax refund claimed by individuals in the form of a loan. Typically the loan amount would include the tax return preparation cost, other fees, and a finance charge.

That work highlighted areas of concern related to the FDIC's supervisory actions that caused banks to exit that business line and prompted frank discussions with FDIC management and the Corporation's Board of Directors. We reported that in our view, the FDIC must candidly consider its leadership practices, its process and procedures, and the conduct of multiple individuals who made and implemented the decision to require banks to exit RALs. While we acknowledged that the events described in our report surrounding RALs involved only three of the FDIC's many supervised institutions, the severity of the events warranted such consideration.

Because our work was in the nature of a review, and not an audit conducted in accordance with government auditing standards, we did not make formal recommendations in the RALs report. However, we requested that the FDIC report to us, 60 days from the date of our final report, on the steps it would take to address the matters raised for its consideration.

On March 16, 2016, the Acting IG testified before the Committee on Financial Services, Subcommittee on Oversight and Investigations, U.S. House of Representatives, and presented the results of the OIG's inquiry into the RALs matter.

The Corporation's responses—from both FDIC management and the FDIC Board of Directors during the previous semiannual reporting period were included in our last report. During June and July 2016, we engaged in further discussions with both management and the FDIC Board, culminating in a final response package provided to the OIG on July 15, and a July 19, 2016 Board of Directors meeting, during which the report's matters for consideration and the FDIC's response to those matters were discussed. Subsequent to the Board meeting, in August, we received a final set of materials from the FDIC outlining specific actions it had committed to take.

Following are the actions relative to four key areas of concern, as outlined in the Executive Summary and corresponding materials provided to our office in August 2016.

Actions to address the clarity and sufficiency of parameters applied to the use of moral suasion, or its equivalents:

To ensure FDIC supervisory expectations are transparent, clear and documented, the Board adopted two Statements of the FDIC Board of Directors:

- *Statement of the FDIC Board of Directors on the Development and Review of Supervisory Guidance (Board approved)*
- *Statement of the FDIC Board of Directors on the Development and Communication of Supervisory Recommendations (Board approved)*

The Corporation also noted the issuance of additional guidance:

- *Issuance of Internal Guidance Regarding Communication with Bankers*
- *Issuance to the Industry - Examination Guidance on Third-Party Lending (To be issued for public comment)*

Actions relative to the adequacy of existing vehicles for examiners and other employees to report what they believe to be inappropriate actions or direction:

The Board adopted the following:

- *Statement of the FDIC Board of Directors on the FDIC Code of Conduct (Board approved)*

Additionally, the Corporation noted the following:

- *Issuance of internal guidance to update the Case Manager Procedures Manual and National Review Examiner Manual to require review at a higher level than normal when an examiner's ratings are changed and the examiner does not concur*
- *Issuance of internal guidance updating RMS Regional Director Delegations of Authority*
- *Statement of Corporate Governance for Supervisory Matters within RMS*
- *Annual Review of Ratings Changes*

Actions relative to the effectiveness and timeliness of avenues of redress available to banks that believe supervisory powers are not used appropriately:

The Board adopted amendments to the Supervision Appeals Review Committee Guidelines, as follows:

- *Update to Supervision Appeals Review Committee Guidelines (Board approved – to be issued for public comment)*
- *Update of Internal Guidance on Requests for Review by the Division Directors*
- *Issuance of External Guidance Regarding the Handling of Disagreements about Examination Findings and Other Matters*

Actions relative to the governance and procedures of the Board and its committees:

The FDIC Board committed to undertake a review of the governance and procedures of the Board and its committees. To clarify the role of the FDIC Board, the FDIC Chairman, and the other Board members in bank supervisory matters and to promote awareness of the Board's Major Matters Resolution, the Board addressed the following:

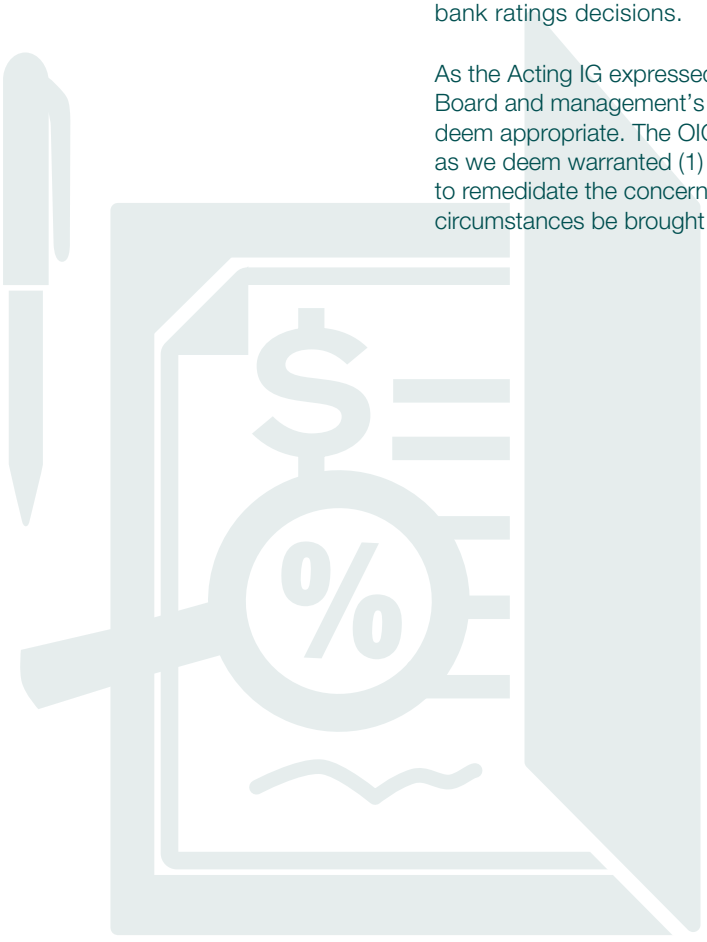
- *Statement of the FDIC Board of Directors on FDIC Corporate Governance for Supervisory Matters (Board approved)*
- *Standing Committee Resolution (Board approved)*

Outside Legal Review of the Actions of Certain Personnel

Finally, with respect to the FDIC's review of the actions of certain personnel, the FDIC's Legal Division engaged outside counsel (Baker Hostetler) to review the Report of Inquiry, the underlying documents, and certain other relevant information and prepare a report analyzing: (1) whether adverse personnel actions against certain current or former FDIC employees were appropriate and warranted based on the circumstances described in the final Report of Inquiry and (2) whether enhancements to FDIC policies and procedures regarding employee performance and conduct may be warranted.

The outside counsel's report concluded that it did not appear any sustainable adverse employment action could be maintained against any specific individual FDIC employee as in its opinion, none of the conduct described in the Report of Inquiry appeared to present a sufficient basis for adverse employment action in light of the overall circumstances. With respect to whether enhancements to FDIC policies and procedures regarding conduct may be warranted based on the facts described in the final Report of Inquiry, the outside counsel report suggested that the FDIC may want to explore whether there is sufficient clarity around the appropriate role of the Washington Office employees in specific bank ratings decisions.

As the Acting IG expressed at the July 19, 2016 FDIC Board meeting, it is the Board and management's responsibility to implement proposed changes as they deem appropriate. The OIG will, in its oversight capacity, conduct further reviews, as we deem warranted (1) to evaluate the effectiveness of steps the FDIC has taken to remedidate the concerns raised in our report and (2) should additional facts or circumstances be brought to our attention that we believe warrant such oversight.



Goal 2: Impactful Investigations

Investigate criminal activities affecting financial institutions and conduct other investigative activities to ensure integrity in the banking industry and FDIC internal operations

The OIG's OI works closely with FDIC management in RMS, DRR, and the Legal Division to identify and investigate financial institution crime, especially various types of bank fraud. OIG investigative efforts are concentrated on those cases of most significance or potential impact to the FDIC and its programs. The goal, in part, is to bring a halt to the fraudulent conduct under investigation, protect the FDIC and other victims from further harm, and assist the FDIC in recovery of its losses. Pursuing appropriate criminal penalties not only serves to punish the offender but can also deter others from participating in similar crimes. In the case of bank closings where fraud is suspected, our OI may send case agents and computer forensic special agents from the Electronic Crimes Unit to the institution. Electronic Crimes Unit agents use special investigative tools to provide computer forensic support to OIG investigations by obtaining, preserving, and later examining evidence from computers at the bank.

Importantly, our criminal investigations can also be of benefit to the FDIC in pursuing enforcement actions to prohibit offenders from continued participation in the banking system. When investigating instances of financial institution fraud, the OIG also defends the vitality of the FDIC's examination program by investigating associated allegations or instances of criminal obstruction of bank examinations and by working with U.S. Attorneys' Offices to bring these cases to justice. The OIG also continues to coordinate with the FDIC's RMS Bank Secrecy Act/Anti-Money Laundering Section to address areas of concern, and we communicate regularly with the DOJ's Asset Forfeiture and Money Laundering Section.

The OIG's investigations of financial institution fraud historically constitute about 90 percent of the OIG's investigation caseload. The OIG is also committed to continuing its involvement in interagency forums addressing fraud. Such groups include national and regional bank fraud, check fraud, mortgage fraud, anti-phishing, and suspicious activity review working groups, as illustrated later in this section. Most recently, and as discussed in detail under goal 4 of this report, the OIG, and OI in particular, has expanded its involvement in several cyber security-related working groups, namely the National Cyber Investigative Joint Task Force and the FBI Washington Field Office Cyber Task Force.

Of note during the reporting period, OI and Counsel's Office helped plan the FDIC and DOJ's Financial Crimes Conference, assisting in developing the 3-day agenda and participating in three presentations. In the first, the Assistant Inspector General for Investigations moderated a panel on IG Perspectives. Additionally, an OI special agent joined the Assistant U.S. Attorney from the Northern District of California and colleagues from the FDIC, in presenting results of a case involving fraud at the failed United Commercial Bank. In another session, the Acting IG and a senior investigative advisor from the OIG joined a representative from DOJ's Office of Foreign Litigation, Civil Division, in discussing trends, developments, and coordination to combat cross-border fraud.

OIG Work in Support of Goal 2

The cases discussed below are illustrative of some of the OIG's most important investigative success during the reporting period. These cases reflect the cooperative efforts of OIG investigators, FDIC divisions and offices, U.S. Attorneys' Offices, and others in the law enforcement community throughout the country.

Our cases during the reporting period include those involving bank fraud, wire fraud, obstruction of an examination, embezzlement, and mortgage fraud. Many of our bank fraud cases involve former senior-level officials, other bank employees, and customers at financial institutions who exploited internal control weaknesses and whose fraudulent activities harmed the viability of the institutions and ultimately contributed to losses to the DIF. Real estate developers and agents, attorneys, and other individuals involved in residential and commercial lending activities were also implicated in a number of our cases. The cases discussed below were conducted by the OIG's special agents in our headquarters and regional offices and reflect nationwide activity and results. The OIG's working partnerships with the Corporation and law enforcement colleagues in all such investigations contribute to ensuring the continued safety and soundness of the nation's banks and help ensure integrity in the FDIC's programs and activities.

Three Former Bank Employees Sentenced for Conspiring to Steal over $3.9 Million from a Bank's Vault

On September 29, 2016, a bank teller at the First National Bank of Lawrence County, Walnut Ridge, Arkansas, was sentenced to serve 57 months in prison, and a head teller and assistant cashier at the bank was sentenced to serve 51 months in prison. The two were also each ordered to pay $1,317,000 in restitution and serve 36 months of supervised release upon their release from prison. On September 30, 2016, a senior vice president and cashier at the bank was sentenced to serve 57 months in prison to be followed by 36 months of supervised release. She was also ordered to pay $1,317,000 in restitution for a combined total of $3,951,000 in restitution from the three defendants. They had all previously pleaded guilty to a criminal Information charging them with conspiracy to commit bank fraud. The defendants were each employed for more than 35 years by the bank in Walnut Ridge, Arkansas, an Office of the Comptroller of the Currency (OCC)-regulated institution.

Beginning from about 2005 and continuing through April 2015, the three women used their positions and acted together to conceal their theft of over $3.9 million from the bank's vault. The theft was first suspected when internal office messages and email logs were discovered among the three subjects during an on-site audit by BKD, LLP in April 2015. The subjects were discussing what could be done to keep the auditors from counting the vault cash. The suspicious messages were shared with the bank's chief executive officer (CEO), who requested BKD to conduct an immediate audit, and BKD subsequently determined the bank's vault cash was short over $3.9 million. The subjects later admitted to their theft during interviews with agents.

> ***Source:*** *First National Bank of Lawrence County, Walnut Ridge, Arkansas.*
> ***Responsible Agencies:*** *This was a joint investigation by FDIC OIG and the FBI. The case was prosecuted by the U.S. Attorney's Office for the Eastern District of Arkansas.*

Former Bank Chairman Found Guilty by Jury

On July 1, 2016, after hearing evidence for 7 days and deliberating approximately 7 hours, a federal trial jury found the former president and chairman of the board of First State Bank of Altus, Altus, Oklahoma, guilty on 10 charges of bank fraud, conspiracy to commit bank fraud, misapplication of bank funds, making a false bank entry, and unauthorized issuance of a bank loan. He could face up to 30 years in prison and a fine of $1 million for each of the 10 counts of conviction.

First State Bank of Altus was closed by the Oklahoma State Banking Department on July 31, 2009, and the FDIC was appointed Receiver. On April 14, 2016, a businessman pleaded guilty to one count of conspiring with the former bank officer to commit bank fraud. He will face up to 5 years in prison.

The two engaged in various loan schemes to finance their personal business activities involving real estate development, senior life insurance settlements, and loans to a start-up company in which both men had ownership interests in order to obtain loan proceeds of over $14 million without proper authorization or approval.

Source: *FDIC RMS.*
Responsible Agencies: *This is a joint investigation with the FBI. The case is being prosecuted by the U.S. Attorney's Office for the Western District of Oklahoma.*

Former Bank Officer Sentenced for Bank Fraud

On July 7, 2016, the former vice president of Mechanics Bank, Water Valley, Mississippi, was sentenced to serve 24 months in prison to be followed by 5 years of supervised release and ordered to pay restitution of $3,346,719 following his February 25, 2016, guilty plea to bank fraud.

From August 2013 through April 2014, the former vice president misused his position and manipulated bank account records to make unauthorized extensions of credit for the benefit of certain bank customers and conceal his activity from the bank's officers and board of directors. He issued fraudulent letters of credit, forged signatures on loan documents and check endorsements, and created nominee loans. In addition, he embezzled funds from Mechanics Bank for his personal benefit.

Source: *FDIC-OIG initiated.*
Responsible Agencies: *This investigation was conducted by the FDIC OIG with the assistance of the U.S. Department of Agriculture OIG. The case is being prosecuted by the U.S. Attorney's Office for the Northern District of Mississippi.*

Former Bank President Pleads Guilty to Conspiracy to Commit Bank Fraud

On May 9, 2016, the former president and CEO of Central Bank, Savannah, Tennessee, pleaded guilty to a criminal Information charging him with one count of conspiracy to commit bank fraud. Sentencing is set for January 12, 2017.

Between March 2009 and February 2012, the former bank president and CEO issued fraudulent letters of credit on behalf of a bank customer and his associated entities, including Tennessee Materials Corporation, to Wayne County Bank, Waynesboro, Tennessee, and First Metro Bank, Muscle Shoals, Alabama, totaling almost $4 million. These letters of credit were issued without authority, were not recorded on the bank's books and records, and were concealed from the bank's board of directors and regulators. The former bank officer also allowed Tennessee Materials Corporation to maintain an overdrawn demand deposit account in excess of $3.9 million by depositing 161 insufficient checks, totaling over $116 million, drawn on other banks for immediate credit in an effort to conceal the overdrafts. Loss to the victim banks is approximately $10 million.

Source: *Central Bank, Savannah, Tennessee.*
Responsible Agencies: *This was a joint investigation conducted by the FDIC OIG and FBI. The case is being prosecuted by U.S. Attorney's Office for the Western District of Tennessee.*

Former United Commercial Bank (UCB)/UCB Holdings, Inc. Senior Vice President Sentenced

On August 30, 2016, a former senior vice president of United Commercial Bank was sentenced to 5 years of probation, 100 hours of community service, and ordered to pay a fine of $4,000 for his role in a securities/bank fraud scheme stemming from the failure of United Commercial Bank. Previously, he agreed to plead guilty to conspiracy to make false bank entries, reports, and transactions.

The former senior vice president conspired with others to manipulate the bank's books and records in a manner that misrepresented and concealed the bank's true financial condition and performance and caused the bank to issue materially false and misleading financial statements for the third quarter of 2008 (10Q and Call Report), and year-end 2008 (10K and Call Report). He assisted the chief credit officer in preparing the quarterly allowance for loan losses report, in which the bank formally calculated the loan loss reserves it was required to recognize as part of its quarterly and annual financial reporting. At the time, the former senior vice president knew the allowance for loan losses report, along with the quarterly call reports and forms 10Q, and 10K for the third quarter 2008 and the year end 2008 were false and misleading.

Source: *In May 2009, UCB Holdings made a public announcement that an internal investigation was initiated and its 2008 year-end financial statements could not be relied on. Once the results of the internal investigation were disclosed to the Board of Directors, the Board of Directors reported the results of the internal investigation to DOJ.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, FRB and Consumer Financial Protection Bureau OIG, and the Special Inspector General for the Troubled Asset Relief Program.*

Former Employee of the FDIC and the Federal Reserve Bank of San Francisco Sentenced

On June 14, 2016, a former employee of the FDIC and the Federal Reserve Bank of San Francisco was sentenced to time served, 1 year of supervised release, 200 hours of community service, and ordered to pay a fine of $4,000 for his false statements for the purpose of influencing an action of the FDIC and a false statement to the Board of Governors of the Federal Reserve System.

Beginning in October or November 2012, the former employee, a principal of Redwood Equity Partners, Inc. who was then an examiner of the Federal Reserve Bank of San Francisco, initiated an effort to purchase America California Bank, San Francisco, California. In February 2013, the former employee failed to disclose on his uniform disclosure form for supervision and regulation personnel, also known as Form D, his position as a director in Redwood Equity Partners, Inc. In January 2014, he prepared and signed an interagency biographical and financial report, which was part of a bank merger application reviewed by the FDIC. In that report, he made several false statements in an effort to influence the FDIC.

Source: *RMS.*
Responsible Agencies: *This was a joint investigation by the FDIC OIG and the FRB and Consumer Financial Protection Bureau OIG. The case is being prosecuted by the U. S. Attorney's Office, Northern District of California.*

Morgan Stanley Financial Advisor Pleads Guilty

On April 27, 2016, a former financial advisor for Morgan Stanley pleaded guilty to conspiracy to commit wire fraud. The former advisor was a licensed securities dealer at the Tucson, Arizona, office of Morgan Stanley. One of his clients had a portfolio loan account with Morgan Stanley Bank, NA, Salt Lake City, Utah. The advisor's brother was the vice president of lending for The Bank of Oswego, Lake Oswego, Oregon. The two brothers convinced the client to invest $1,000,000 in a transaction to fund an entity controlled by the advisor's brother for the purchase of three condominiums in Palm Springs, California. The client was to receive an interest in each of the three condominiums as security for her investment; however, the advisor's brother resold two of the properties without repaying her. The brothers further conspired to involve the client in a transaction whereby her Morgan Stanley NA portfolio loan account funded a $2,000,000 transaction that benefitted the advisor's brother and repaid an outstanding loan at The Bank of Oswego. The advisor conducted the transaction using a previously signed wire authorization when, in fact, the client never authorized the $2,000,000 transaction.

> ***Source:*** *RMS and the FBI.*
> ***Responsible Agencies:*** *This is a joint investigation by the FDIC OIG and the FBI. The case is being prosecuted by the U.S. Attorney's Office for the District of Oregon.*

Broker Sentenced for Lying to Investigators and Obstructing La Jolla Bank Bribery Investigation

On August 15, 2016, a loan broker for La Jolla Bank, La Jolla, California, was sentenced to time served; 3 years of supervised release; and ordered to pay restitution of $82,185 to the Small Business Administration (SBA) and the FDIC. She was sentenced for making false statements to federal agents regarding her role in a bank bribery case.

According to the plea agreement, the former broker worked as an unofficial broker for La Jolla Bank, referring business loan customers to the bank's SBA department. As part of this job, she helped her borrowers compile their loan application packages and submit them to the bank. In return for generating business, La Jolla Bank paid her a commission or referral fee, calculated as a percentage of each loan she referred. She admitted that in 2006, an SBA loan manager asked her to kick back a portion of her commissions, in cash, after her clients' loans were funded. In turn, the SBA loan manager would make sure that the broker's clients' loans were approved so that the broker could collect commission payments, regardless of the soundness of the loans and their benefit to the bank. In addition, the SBA loan manager arranged to pay her a fraudulent $30,000 "commission" for a loan she in fact had no part in brokering. The loan broker went so far as to generate a fake invoice, pretending that she had earned the commission.

She further admitted that she lied to law enforcement agents by concealing these bribe payments and hiding her relationship with the SBA loan manager. During the investigation, she told federal agents, falsely, that she never saw the SBA loan manager accept money in exchange for loans. Further, despite the fact that she and the SBA loan manager traded several phone calls and text messages and had a sit-down meeting in June 2014, she falsely reported to federal agents in September 2014 that she had not spoken to or seen the former loan manager since before she learned about the federal investigation. In her plea agreement, she acknowledged that her false statements significantly impeded the investigation of the SBA loan manager.

The SBA loan manager has pleaded guilty to accepting bribes, and admitted that she and other senior La Jolla Bank executives accepted hundreds of thousands of dollars in cash bribes and kickbacks from borrowers in return for issuing hundreds of millions of dollars in loans. The bank management issued the loans knowing that the borrowers were unqualified and unlikely to repay, and their mismanagement contributed to the bank's billion-dollar collapse. The SBA loan manager admitted that she participated in a conspiracy with the bank's senior executives to line their own pockets with bribe money. She was sentenced on August 22, 2016, as discussed further in the following write-up.

Source: *SBA OIG.*
Responsible Agencies*: This is a joint investigation by the FDIC OIG, FBI, Federal Housing Finance Agency (FHFA) OIG, SBA OIG, and Treasury Inspector General for Tax Administration. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of California.*

La Jolla Bank Manager Sentenced for Conspiracy to Misapply Bank Funds

On August 22, 2016, an SBA loan manager was sentenced to time served; 12 months of home detention; 3 years of supervised release; and ordered to pay restitution in the amount of $1,456,073 for conspiring to misapply bank funds while managing the SBA lending department of La Jolla Bank, La Jolla, California, from 2005 until 2009.

In 2005, La Jolla Bank opened its SBA department. The SBA loan manager did not have authority to lend bank funds, but instead reviewed borrowers' applications and recommended that loans be approved. The loan manager required approval from either the bank's CEO or the chief credit officer before funds were disbursed. These two bank officers and other bank employees offered favorable terms and treatment to certain high-volume borrowers to whom they referred as "Friends of the Bank." The bank officers encouraged the SBA loan manager to offer the same favorable terms and treatment to SBA borrowers.

From 2005 until 2009, the three bank insiders and others would cause the bank to issue loans under favorable terms to unqualified or under-qualified Friends of the Bank and SBA borrowers, in order to personally enrich themselves, knowing that these disbursements served no benefit to the bank and intending to injure and defraud the bank. The conspirators would support the disbursement of bank funds by supplying or knowingly accepting false and fraudulent information in the borrowers' loan applications, and would knowingly overlook negative aspects of the borrowers' creditworthiness. They would demand and accept personal payments from the borrowers, in return for loans issued by the bank. They would use the loan disbursements to inflate the bank's performance measures, which in turn would increase their compensation from the bank. In order to prevent these risky loans from going into default and exposing the true poor performance of the bank's receivables, the conspirators would cause the bank to issue additional loans, including extensions of lines of credit, to enable the borrowers to make loan payments.

As part of the conspiracy, the two bank officers arranged for the bank to issue hundreds of millions of dollars in loans to unqualified or under-qualified Friends of the Bank. Many of these loans defaulted, contributing to the failure of the bank. Also as part of the conspiracy, and at the direction of the two officers, the SBA loan manager arranged for the bank's SBA department to issue at least $55.8 million in loans to largely unqualified or under-qualified SBA borrowers. As a result, the bank was deprived of control over its funds and suffered losses within the SBA department alone of approximately $19.8 million.

Source: *SBA OIG.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FBI, FHFA OIG, SBA OIG, and Treasury Inspector General for Tax Administration. The case is being prosecuted by the U.S. Attorney's Office for the Southern District of California.*

Bank Customer Pleads Guilty in Bank Fraud Scheme

On August 25, 2016, the owner and president of Machine Tools Direct, Inc. (MTD), pleaded guilty to bank fraud. He and a business partner were indicted on February 27, 2014, in a 10-count indictment charging them with mail fraud, bank fraud and wire fraud. The president of MTD will be sentenced on December 1, 2016.

Between early 2006 and October 2009, the MTD president and the former president and co-owner of Equipment Acquisition Resources, Inc., (EAR) engaged in a scheme to fraudulently obtain approximately $190 million from banks and financing companies, eventually causing those lenders to lose at least $100 million. The MTD president used false representations about MTD's business operations, financial status, independence from EAR, and need for financing when applying for loans. Both business owners falsely represented to lenders that EAR and MTD were separate companies engaged in arms-length sales transactions. The MTD president obtained financing for his company to purchase equipment from EAR, and he and EAR's president arranged sham sales transactions between the two companies. After MTD received financing from the lenders, the MTD president sent most of the proceeds to the EAR president so that EAR could use the money to make payments on other loans. The EAR president pleaded guilty in January 2015 and on July 22, 2015, was sentenced to 60 months in prison.

Source: *Request for assistance from the FBI.*
Responsible Agencies: *The FDIC OIG is conducting the investigation jointly with the FBI. This case is being prosecuted by the U.S. Attorney's Office for the Northern District of Illinois.*

Former Bank Official Sentenced for Bank Fraud

On August 15, 2016, the former Vice President of Citizens First National Bank (CFNB), Princeton, Illinois, was sentenced to 2 months in prison, 6 months of home confinement, and 60 months of supervised release. He was also ordered to pay $55,000 in restitution to the FDIC. CFNB was an OCC-regulated financial institution. The FDIC was named Receiver when CFNB was closed on November 2, 2012.

From 2002 through 2011, the former president personally borrowed monies from bank customers (in excess of $200,000), much of which was never repaid. The personal loans were in violation of CFNB's Code of Conduct policy, which he was required to certify on an annual basis. Further, during the period in question, the former bank president applied for personal loans totaling in excess of $80,000, with CFNB and State Bank of Paw Paw, Earlsville, Illinois, and never disclosed the existence of the $200,000 in unpaid personal loans during the process of obtaining the loans from the banks. The loans resulted in losses to both financial institutions.

Source: *DRR.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG and the Special Inspector General for the Troubled Asset Relief Program. The case is being prosecuted by the U.S. Attorney's Office, Central District of Illinois.*

Mortgage Fraud Schemer Sentenced in Detroit

On February 20, 2014, a mortgage fraud schemer pleaded guilty to conspiracy to commit bank fraud. He was previously charged in an Indictment along with a former vice president of the Bank of Michigan, Farmington Hills, Michigan, for their roles in a mortgage fraud conspiracy. On July 16, 2014, the mortgage fraud schemer was sentenced to serve 20 months in prison, but on January 14, 2015, he failed to surrender to the U.S. Marshall's Service to begin serving his sentence. A bench warrant was then issued for his arrest. On January 17, 2015, Mexican immigration officials arrested him as he was traveling under the name of another person and turned him over to U.S. Customs and Border Protection. On February 3, 2015, he was indicted by a federal grand jury in Detroit for his failure to surrender for sentence. On August 25, 2016, he was sentenced to time served (17 months).

This case was initiated based on information indicating that the former bank vice president produced a number of fraudulent verifications of deposit on behalf of suspected straw buyers recruited by the mortgage fraud schemer, who in turn paid the bank president for the verifications. The false verifications were used in a series of fraudulent mortgage transactions affecting Washington Mutual, FSB, Countrywide, and other financial institutions.

Source: *RMS and the FBI.*
Responsible Agencies: *This was a joint investigation by the FDIC OIG and the FBI and was prosecuted by the U.S. Attorney's Office for the Eastern District of Michigan.*

Former Loan Officer Pleads Guilty

On April 19, 2016, a loan officer at Horicon Bank, Horicon, Wisconsin, was indicted on bank fraud and conspiracy charges by the Eastern District of Wisconsin. He pleaded guilty on July 22, 2016 for his role in the conspiracy to defraud the bank.

Between January 2008 and September 2009, the loan officer approved a series of loans for the benefit of a businessman and his wife. In January 2008, the loan officer approved a $250,000 loan to one of the businessman's many companies. He then proposed a $7.1 million loan for Source of Solutions, another of the businessman's companies. Bank management denied this loan and instructed the loan officer not to make any more loans to the businessman or his business entities. The loan officer subsequently made a series of nine loans to nominee borrowers recruited by the businessman. These nominee borrowers did not receive the loan proceeds and did not believe they were responsible for repayment of the loans. The businessman's use of nominee borrowers, coupled with the fact that all of the loans were at or below the loan officer's $250,000 lending limit, caused the true overall relationship between the loans to go unnoticed by bank management. The businessman did not repay the loans and Horicon Bank ended up charging off $713,191.

Source: *RMS.*
Responsible Agencies: *This case is being investigated by the FDIC OIG, FBI, and IRS-CI and is being prosecuted by the U.S. Attorney's Office for the Eastern District of Wisconsin.*

Former Bank CEO and Holding Company Director Sentenced for Obstruction of an Examination

On May 25, 2016, the former CEO and chairman of Voyager Bank, Eden Prairie, Minnesota, and director of Voyager Financial Services Corporation (VFSC), the bank holding company for Voyager, was sentenced to serve 18 months in prison to be followed by 2 years of supervised release, following his July 30, 2015, guilty plea to obstructing an examination of a financial institution.

From on or about 2004 and continuing through July 2011, the former CEO abused his position with the bank by obtaining $9.7 million in letters of credit and other bank holding company loans that he knew he couldn't repay. He carefully circumvented the bank's and the bank holding company's lending procedures to ensure that his credit extensions were not subject to the full review and approval of the bank's senior management, the board, or the bank holding company's board. The loss to Voyager and to VFSC due to the former CEO's activities is estimated at $15 million. To conceal his illicit acts during and after a regulatory examination of VFSC, he made false and misleading statements to the Federal Reserve Bank of Minneapolis (FRB-MN) in reply to an FRB-MN letter criticizing VFSC's loans to him. By submitting misleading documents, he was able to satisfy the FRB-MN's concerns about his loans, thus allowing the scheme to continue and losses to increase.

Source: *RMS.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, FRB OIG, FHFA OIG, and the FBI and is being prosecuted by the U.S. Attorney's Office for the District of Minnesota.*

Former Bank Employees Sentenced in Bank Fraud Scheme

On April 29, 2016, two former bank employees from two different Minnesota banks, one a branch manager, and the other a teller, were both sentenced to serve 12 months and 1 day in prison to be followed by 3 years of supervised release; each defendant was also ordered to pay $51,161.55 in restitution.

According to the indictment, from at least November 14, 2007, until September 11, 2013, the two and others were participants in a bank fraud scheme. The conspirators fraudulently obtained and otherwise compromised account information, manufactured counterfeit checks with blank check stock and check-printing software, and distributed the counterfeit checks to other members of a bank fraud conspiracy to cash at dozens of different banks and other financial institutions. The three primary counterfeit check manufacturers used various means of obtaining account information to make counterfeit checks, including getting access to sensitive account information through the two bank insiders who facilitated the conspiracy by using their access to legitimate account information to provide the manufacturers with account numbers and balance information.

Source: *Minnesota Financial Crimes Task Force.*
Responsible Agencies: *This is a joint investigation by the Minnesota Financial Crimes Task Force, FDIC OIG, IRS-CI, the United States Postal Inspection Service, the United States Secret Service, and Immigration and Customs Enforcement. The case is being prosecuted by the U.S. Attorney's Office for the District of Minnesota.*

Former Branch Manager Sentenced

On May 31, 2016, the former branch manager, First Home Savings Bank, Mountain Grove, Missouri, was sentenced to serve 1 year in prison to be followed by 5 years of supervised release. She was also ordered to pay restitution in the amount of $211,412.54. On January 27, 2016, she pleaded guilty to one count of making a false entry in a bank's books and one count of filing a false federal income tax return.

From March 13, 2012, through January 3, 2013, the former branch manager misused her position as First Home Savings Bank branch manager to embezzle cash from the bank's vault. To further her scheme, she manipulated the bank's records to try and hide the embezzlement.

Source: *RMS.*
Responsible Agencies: *This is a joint investigation by the FDIC OIG, the FBI, and IRS-CI. The case is being prosecuted by the U.S. Attorney's Office for the Western District of Missouri.*

Electronic Crimes Unit Responds to Email and Other Schemes

The Electronic Crimes Unit (ECU) continues its work to identify and mitigate the effects of phishing attacks through emails claiming to be from the FDIC. These schemes persist and seek to elicit personally identifiable and/or financial information from their victims. The nature and origin of such schemes vary, and, in many cases, it is difficult to pursue the perpetrators, as they are quick to cover their cyber tracks, often continuing to originate their schemes from other Internet addresses and from locations outside of the U.S.

In prior semiannual reports, we noted that the ECU learned that over 20 individuals in foreign countries were contacted by individuals claiming to be from the FDIC's DRR. The foreign individuals were fraudulently informed that the FDIC was going to reimburse them for stock losses after they paid fees to release the funds. The ECU informed the foreign individuals that these types of contacts are fraudulent. We noted that other government agencies may have been victimized by the same group in this international investment scam. During the reporting period, we learned that additional parties have been contacted by individuals claiming FDIC affiliation and soliciting personally identifiable information as proof that the party is entitled to a return. The ECU continues to coordinate with the FBI, Treasury Inspector General for Tax Administration, Department of the Treasury OIG, Internal Revenue Service, and Securities and Exchange Commission OIG on such cases.

Strong Partnerships with Law Enforcement Colleagues

The OIG has partnered with various U.S. Attorneys' Offices throughout the country in bringing to justice individuals who have defrauded the FDIC or financial institutions within the jurisdiction of the FDIC, or criminally impeded the FDIC's examination and resolution processes. The alliances with the U.S. Attorneys' Offices have yielded positive results during this reporting period. Our strong partnership has evolved from years of hard work in pursuing offenders through parallel criminal and civil remedies resulting in major successes, with harsh sanctions for the offenders. Our collective efforts have served as a deterrent to others contemplating criminal activity and helped maintain the public's confidence in the nation's financial system.

During the reporting period, we partnered with U.S. Attorneys' Offices in the following areas: Alabama, Arizona, Arkansas, California, Colorado, District of Columbia, Florida, Georgia, Idaho, Illinois, Indiana, Iowa, Kansas, Kentucky, Louisiana, Maryland, Massachusetts, Michigan, Minnesota, Mississippi, Missouri, Nebraska, Nevada, New Jersey, New Mexico, New York, North Carolina, North Dakota, Ohio, Oklahoma, Oregon, Pennsylvania, South Carolina, South Dakota, Tennessee, Texas, Utah, Vermont, Virginia, Washington, West Virginia, Wisconsin, and Puerto Rico.

We also worked closely with the Department of Justice; FBI; other OIGs; other federal, state, and local law enforcement agencies; and FDIC divisions and offices as we conducted our work during the reporting period.

OIG Shares Perspectives

At the FDIC's 2016 Financial Crimes Conference, from left to right: Special Agent Kelvin Zweifelhofer participates on a panel presenting a case study of United Commercial Bank. Acting IG Fred Gibson and Senior Investigative Advisor Gary Sherrill discuss challenges in combating cross-border fraud.

NY Region Special Agent in Charge Patti Tarasca presents Park Avenue Bank case at the FDIC's 2016 Accounting and Auditing Conference.

Keeping Current with Criminal Activities Nationwide

The FDIC OIG participates in the following bank fraud, mortgage fraud, cyber fraud, and other working groups and task forces throughout the country. We benefit from the perspectives, experience, and expertise of all parties involved in combating criminal activity and fraudulent schemes nationwide.

OIG Headquarters	Financial Fraud Enforcement Task Force, National Bank Fraud Working Group — National Mortgage Fraud Working Sub-group.
New York Region	New York State Mortgage Fraud Working Group; Newark Suspicious Activity Report (SAR) Review Task Force; Philadelphia SAR Review Team; El Dorado Task Force - New York/New Jersey HIDTA; Philadelphia Financial Exploitation Prevention Task Force; Maryland Mortgage Fraud Task Force; Philadelphia Mortgage Fraud Working Group; Pittsburgh SAR Review Team.
Atlanta Region	Middle District of Florida Mortgage and Bank Fraud Task Force; Southern District of Florida Mortgage Fraud Working Group; Northern District of Georgia Mortgage Fraud Task Force; Eastern District of North Carolina Bank Fraud Task Force; Northern District of Alabama Financial Fraud Working Group; Northern District of Georgia SAR Review Team; Middle District of Georgia SAR Review Team; South Carolina Financial Fraud Task Force.
Kansas City Region	St. Louis Mortgage Fraud Task Force; Kansas City Financial Crimes Task Force; Minnesota Inspector General Council meetings; Minnesota Financial Crimes Task Force; Kansas City SAR Review Team; Springfield Area Financial Crimes Task Force; Nebraska SAR Review Team; Iowa Mortgage Fraud Working Group.
Chicago Region	Dayton, Ohio, Area Financial Crimes Task Force; Illinois Fraud Working Group; Central District of Illinois SAR Review Team; Detroit SAR Review Team; Financial Investigative Team, Milwaukee, Wisconsin; Milwaukee Mortgage Fraud Task Force; Madison, Wisconsin, SAR Review Team; Indiana Bank Fraud Working Group; FBI Louisville Financial Crime Task Force; U.S. Secret Service Louisville Electronic Crimes Task Force; Western District of Kentucky SAR Review Team.
San Francisco Region	FBI Seattle Mortgage Fraud Task Force; Fresno Mortgage Fraud Working Group for the Eastern District of California; Sacramento Mortgage Fraud Working Group for the Eastern District of California; Sacramento SAR Working Group; Los Angeles Mortgage Fraud Working Group for the Central District of California; Orange County Financial Crimes Task Force-Central District of California.
Dallas Region	SAR Review Team for Northern District of Mississippi; SAR Review Team for Southern District of Mississippi; Oklahoma City Financial Crimes SAR Review Working Group; Austin SAR Review Working Group.
Electronic Crimes Unit	Washington Metro Electronic Crimes Task Force; Botnet Threat Task Force; High Technology Crime Investigation Association; Cyberfraud Working Group; Council of the Inspectors General on Integrity and Efficiency Information Technology Subcommittee; National Cyber Investigative Joint Task Force; FBI Washington Field Office Cyber Task Force.

Goal 3: Effective Communications

Communicate Effectively with Internal and External Stakeholders

Strong working relationships are fundamental to our success. In that regard, effective communications with OIG stakeholders both internal and external to the Corporation are vital. During the reporting period, in addition to focusing on our own staff as a primary stakeholder in our office, we examined the information needs of the OIG's many other stakeholders, including the FDIC Board of Directors and FDIC division and office management and their staffs, the Congress, members of the IG community, GAO, OMB, the media, and the general public.

Importantly, we keep OIG staff informed of office priorities and key activities. We do so through regular meetings among staff and management, bi-weekly updates from senior management meetings, and issuance of OIG newsletters. During the reporting period we received the results of the Federal Employee Viewpoint Survey and have considered the implications of the survey responses from OIG staff to our office culture. We also place a high priority on maintaining positive working relationships with the FDIC Chairman, Vice Chairman, other FDIC Board members, and management officials. The OIG is a regular participant at FDIC Board meetings and at Audit Committee meetings where recently issued audit and evaluation reports are discussed. Other meetings occur throughout the year as OIG officials confer with division and office leaders and attend and participate in internal FDIC conferences and other forums.

Equally, the OIG places a high priority on maintaining positive relationships with the Congress and providing timely, complete, and high-quality responses to congressional inquiries. In most instances, this communication would include semiannual reports to the Congress; issued audit and evaluation reports; responses to other legislative mandates; information related to completed investigations; comments on legislation and regulations; written statements for congressional hearings; contacts with congressional staff; responses to congressional correspondence and Member or Committee requests; and materials related to OIG appropriations.

The OIG fully supports and participates in IG community activities through CIGIE. We coordinate closely with representatives from the other financial regulatory OIGs. In this regard, the Dodd-Frank Act created the Financial Stability Oversight Council and further established CIGFO. This Council facilitates sharing of information among CIGFO member Inspectors General and discusses ongoing work of each member IG as it relates to the broader financial sector and ways to improve financial oversight. CIGFO may also convene working groups to evaluate the effectiveness of internal operations of the Financial Stability Oversight Council.

Additionally, the OIG meets with representatives of the GAO to coordinate work, provide OIG perspectives on risk, and minimize duplication of effort. Similarly we coordinate with the OMB on budgeting and other matters requiring OIG attention. As noted earlier in this report, we also work closely with representatives of the DOJ, including the FBI and U.S. Attorneys' Offices, to coordinate our criminal investigative work and pursue matters of mutual interest.

With respect to public stakeholders interested in our office and/or who contact the OIG for information or assistance, the OIG's inquiry intake system supplements the OIG Hotline function. The Hotline continues to address allegations of fraud, waste, abuse, and possible criminal misconduct. However, over the past several years, our office has continued to receive a large number of public inquiries ranging from media inquiries to requests for additional information on failed institutions to pleas for assistance with mortgage foreclosures to questions regarding credit card companies and banking practices. These inquiries come by way of phone calls, emails, faxes, and other correspondence. The OIG captures and tracks all inquiries in a system known as QUEST and makes every effort to acknowledge each inquiry and be responsive to the concerns raised. We coordinate closely with others in the Corporation who field inquiries and concerns from the public and appreciate their assistance in responding to those who contact our office. We handle those matters within the OIG's jurisdiction and refer inquiries, as appropriate, to other FDIC offices and units or to external organizations.

Importantly, during the reporting period, in recognition of the important role that whistleblowers play in reporting waste, fraud, and abuse and in saving taxpayer dollars and serving the public interest, the Senate passed a resolution designating July 30, 2016 as National Whistleblower Appreciation Day. In this regard, FDIC Chairman Gruenberg issued a global email supporting whistleblowers and advising them of the appropriate channels for reporting their concerns.

Whistleblowers can approach the OIG in a number of ways. Perhaps the most common vehicle for whistleblowers to contact us is through our Hotline. Alternatively, whistleblowers can contact OIG staff directly to inform them of concerns. The OIG's Whistleblower Protection Ombudsman's role is to educate FDIC employees about prohibitions on retaliation for protected disclosures, and educate FDIC employees who have made or are contemplating making a protected disclosure about the rights and remedies against retaliation for protected disclosures.

Our office is pursuing a related certification through the Office of Special Counsel, and training will be provided to OIG staff so that we are all aware of the proper steps to take to ensure that whistleblowers continue to feel free to report their concerns without retaliation.

OIG Work in Support of Goal 3

During the reporting period, we maintained open communication channels with stakeholders, as follows:

FDIC Board, Management, and Staff:

- Communicated with the Chairman, Vice Chairman, other FDIC Board Members, the Chief Financial Officer, and other senior FDIC officials through the Acting IG's regularly scheduled meetings with them and through other forums.

- Held quarterly meetings with FDIC Division Directors and other senior officials to keep them apprised of ongoing OIG reviews, results, and planned work.

- Kept RMS, DRR, the Legal Division, and other FDIC program offices informed of the status and results of our investigative work impacting their respective offices. This was accomplished by notifying FDIC program offices in headquarters and the regional offices of recent actions in OIG cases and providing OI's quarterly reports to RMS, DRR, and the Legal Division outlining activity and results in our cases involving closed and open banks. Coordinated closely with the Legal Division on matters pertaining to enforcement actions and professional liability cases.

- Coordinated with the FDIC Vice Chairman, in his capacity as Chairman of the FDIC Audit Committee, to provide status briefings and present the results of completed audits, evaluations, and related matters for his and other Committee members' consideration.

- Coordinated with DOJ and U.S. Attorneys' Offices throughout the country in the issuance of press releases announcing results of cases with FDIC OIG involvement and routinely informed the FDIC's Office of Communications and Chairman's Office of such releases.

- Attended FDIC Board Meetings, IT/Cyber Security Oversight Group meetings, CIO Council, corporate planning and budget meetings, and other senior-level management meetings to monitor or discuss emerging risks at the Corporation and tailor OIG work accordingly.

- Reviewed six draft FDIC directives and provided substantive comments on proposed policies related to classified national security information, clearances, and potential unauthorized release of such information and other comments regarding acceptable use of IT resources at the FDIC.

- Provided the OIG's view of the management and performance challenge areas that we identified at the FDIC, in accordance with the Reports Consolidation Act of 2000 as we conducted audits, evaluations, and investigations: Carrying Out Dodd-Frank Act Responsibilities, Maintaining Strong IT Security and Governance Practices, Maintaining Effective Supervision and Preserving Community Banking, Carrying Out Current and Future Resolution and Receivership Responsibilities, Ensuring the Continued Strength of the Deposit Insurance Fund, Promoting Consumer Protections and Economic Inclusion, Implementing Workforce Changes and Budget Reductions, and Ensuring Effective Enterprise Risk Management Practices.

The Congress:

- Maintained congressional working relationships by communicating with various Committee staff on issues of interest to them; providing them our semiannual report to the Congress; notifying interested congressional parties regarding the OIG's completed audit and evaluation work; attending or monitoring FDIC-related hearings on issues of concern to various oversight committees; and coordinating with the Corporation's Office of Legislative Affairs on issues of mutual interest.

- More specifically, in addition to the Acting IG's testimonies before the House SST Committee, among other matters, we briefed and/or responded to interested Congressional parties regarding FDIC document productions related to reporting of major information security incidents; an earlier advanced persistent threat event at the FDIC; a situation involving FDIC employee access to OIG email servers; the status of open, unimplemented recommendations; closed audits, evaluations, and investigations that were not made available to the public; and referrals to DOJ and resulting prosecutions. We also informed the Congress that there were no instances where the FDIC delayed or restricted access to records or attempted to interfere with OIG independence; no instances where senior officials' misconduct was found but no prosecution resulted; and no instances of whistleblower retaliation.

- Prepared transition materials with information on the FDIC OIG's organization, role, mission, and impact to be provided to the new Administration and Members of the new Congress following the November 2016 elections.

The IG Community:

- Supported the IG community by attending monthly CIGIE meetings; participating on the CIGIE Audit Committee and the Professional Development Committee (and leading its Human Resources Roundtable); attending Assistant Inspectors General for Investigations, Council of Counsels to the IGs, Federal Audit Executive Council and other meetings; hosting CIGIE's IG Authorities training for those new to the IG community; assisting in the development of a curriculum for CIGIE's Intermediate Auditor Training; participating in the Federal Audit Executive Council's DATA Act Working Group; responding to multiple requests for information on IG community issues of common concern; and commenting on various legislative matters through CIGIE's Legislative Committee.

- Communicated with representatives of the OIGs of the federal banking regulators and others to discuss audit, evaluation, and investigative matters of mutual interest and leverage knowledge and resources.

- Coordinated with representatives from the Federal Trade Commission OIG to share information and discuss issues involving reporting of major information security incidents in our respective agencies.

- Participated on CIGFO, as established by the Dodd-Frank Act, and coordinated with the IGs on that council. Joined others on a CIGFO audit team in a project regarding the Financial Stability Oversight Council's efforts to promote market discipline and provided the FDIC OIG's input to the CIGFO annual report for 2016.

The Government Accountability Office:

- Met with GAO to provide our perspectives on the risk of fraud at the FDIC. We did so in response to GAO's responsibility under Statement of Auditing Standards No. 99, Consideration of Fraud in Financial Statement Audits.

- Coordinated with GAO on its ongoing efforts related to the annual financial statement audit of the FDIC and on other GAO work of mutual interest, including work related to FISMA.

The Public:

- Continued using our QUEST inquiry intake system to capture and manage inquiries from the public, media, Congress, and the Corporation, in the interest of prompt and effective handling of such inquiries. Coordinated with other FDIC divisions and offices to share information on inquiries and complaints received, identify common trends, and determine how best to respond to public concerns. Responded to 225 such inquiries during the past 6-month period.
- Participated in numerous outreach efforts, including providing fraud training for the Federal Financial Institutions Examination Council; speaking on the topic of Integrity at Georgia Southern University's Forensic Accounting Conference; sharing perspectives on succession planning and hiring at an April 2016 Training Officers conference; and speaking to graduate students in Public Administration at Ball State University about law enforcement and the OIG's work investigating various white-collar crimes.
- Maintained contact with representatives from the Deposit Insurance Corporation of Japan regarding the Japanese and U.S. legal and financial systems and their respective approaches for pursuing cases involving failed banks.
- Accepted an invitation from the Department of the Treasury's Office of Technical Assistance to participate in a training program for the Ukrainian Deposit Guarantee Fund and other Ukrainian agencies. The goal of the training is to explain how U.S. authorities investigate bank failure cases and other complex banking investigations, with an emphasis on interagency cooperation on such cases.

Ongoing work at the end of the reporting period in support of this goal included revision of OIG Congressional protocols to update procedures for Congressional activities, participation in the IG community's Public Affairs interest group, research on the use of social media as a tool for communicating OIG work, development of new and more relevant content for the OIG's external Website, and formulation of a more formal media relations function.

Goal 4: Enhanced Understanding of Emerging Issues

Continuously seek to enhance OIG knowledge and understanding of emerging and evolving issues affecting the FDIC, OIG, and insured depository institutions

The FDIC OIG keeps current on emerging issues and threats to the FDIC, our own office, and insured depository institutions. A priority area of focus for the OIG is the evolving issue of cyber security. To enhance the OIG's knowledge and understanding of current and emerging cyber threats to our office, the FDIC, the financial services industry at-large, and other federal entities and operations, we have increased our participation in government-wide task forces and law enforcement working groups, and actively expanded our monitoring and awareness of cyber-related matters. The OIG's Cyber Event Group is designed to identify key resources to ensure the OIG's continuous coverage and readiness to address potentially urgent cyber events affecting the FDIC or other federal entities. Further discussion of our efforts in the cyber-security realm is presented below.

A second area of high importance facing our office relates to the Dodd-Frank Act and the risk of failure of a SIFI. As noted in past semiannual reports, we undertook a risk assessment of the Act in the interest of better understanding its impact on the FDIC and our office. From that assessment, we have completed several reviews and continue to open others. Additionally, a provision in the Dodd-Frank Act could have a substantial bearing on our workload and resources, as along with the failure of a SIFI would come a set of responsibilities for the FDIC OIG as well. Specifically, in the event of a Title II Orderly Liquidation, the OIG would be required to conduct work to address various issues and meet certain reporting requirements based on that work. This challenging area is also discussed below.

OIG Work in Support of Goal 4

FDIC OIG Increases Efforts to Address Cyber Threats

The OIG is tackling threats to the FDIC's IT environment on multiple fronts. One of our senior managers continues to serve as the OIG's Senior Cyber Security Liaison Officer. In that role, he is monitoring cyber-related activities and potential threats both internal and external to the FDIC and disseminating information to mitigate potential risk or harm to the FDIC, the OIG, and insured depository institutions. This same individual represents the OIG at meetings of the Data Breach Management Team for awareness purposes. He is also a member of the Insider Threat and Counterintelligence Program working group. Our interest is to proactively help prevent any release by FDIC insiders—accidental or deliberate—of sensitive information beyond the walls of the FDIC's secure environment—through electronic means such as emailing sensitive information to personal email accounts or otherwise allowing such information to be disclosed without authorization. Others in the OIG play key roles in the IT and cybersecurity arena, to include our information security manager, IT professionals in our Office of Audits and Evaluations, members of our ECU, and a Special Advisor to the Acting IG. Our OIG Cyber Event Group, comprised of many of these individuals, continues to ensure OIG readiness to address cyber threats to the FDIC and share information with interested parties internal and external to the FDIC.

Over the past reporting period, the OIG has also continued its participation in two key cyber-related task forces, in the interest of enhancing our understanding and awareness of current and emerging cyber issues and sharing our own expertise with others seeking to combat cyber threats. These task forces and our involvement are described below. Finally, we also participate in training activities sponsored by the First Information Operations Command of the U.S. Army to better understand the authorities, roles, and responsibilities of the defense and intelligence communities to identify, analyze, and respond to potential cyber threats.

FBI Cyber Task Force

The FBI has established a nationwide network of field office Cyber Task Forces to focus on cybersecurity threats. In addition to key law enforcement and homeland security agencies at the state and local level, each Cyber Task Force partners with many of the federal agencies at the headquarters level. This promotes effective collaboration and de-confliction of efforts at both the local and national level.

In support of the national effort to counter threats posed by terrorist, nation-state, and criminal cyber actors, each Cyber Task Force synchronizes domestic cyber threat investigations in the local community through information sharing, incident response, and joint enforcement and intelligence actions. Each Cyber Task Force leverages the authorities and capabilities of the participating agencies to accomplish the mission.

The FDIC OIG ECU continued its participation in the Washington Field Office Cyber Squad-4 (CY-4). There are 19 other federal, state, and local law enforcement agencies participating in CY-4, which has a total of 56 members. Through participation in CY-4, the ECU assists with new and ongoing FBI and partner cyber investigations by conducting interviews, victim notifications, forensic evidence review, and search warrants. The ECU agents also have access to many FBI informational systems and cyber notifications allowing them to search for relevant data on subjects and entities already under investigation or intrusions at FDIC-insured banks.

Our involvement with the Cyber Task Force has increased our awareness of current threats. As a result of our access to the FBI's systems and other notifications received as a member of the task force, we have opened several investigative inquiries that are currently underway.

National Cyber Investigative Joint Task Force

The National Cyber Investigative Joint Task Force (NCIJTF) is a multi-agency cyber center that serves as the national focal point for coordinating, integrating, and sharing information related to cyber threat investigations. The task force performs its role through the cooperation and collaboration of its co-located 19 partner agencies, its 4 affiliate member agencies, and its on-site representatives from both international partners and state and local law enforcement organizations. Members have access to a unique, comprehensive view of the nation's cyber threat while working together in a collaborative environment in which they maintain the authorities and responsibilities of their home agencies.

The NCIJTF was established in 2008 by National Security Presidential Directive 54/HSPD-23. The responsibility for the task force's development and operation was given to the U.S. Attorney General who entrusted this mission to the FBI. In 2013, the NCIJTF separated from the FBI's cyber operational organization and increased the leadership and participation from its member agencies. Key functions of the NCIJTF include:

- Integrating domestic cyber data
- Coordinating whole-of-government cyber campaigns
- Analyzing and sharing domestic cyber information
- Exploiting financial data to generate new leads and to discover new threats
- Coordinating 24/7 cyber incident threat responses
- Identifying adversaries, compromises, exploit tools, and vulnerabilities
- Informing cyber policy and legislation decision-making

The NCIJTF is led by a Director assigned from the FBI and a Principal Deputy Director assigned from the National Security Agency. Assisting them in the operational direction and tempo of the task force is the NCIJTF Mission Council, comprised of representatives from the National Security Agency, Central Intelligence Agency, U.S. Secret Service, Department of Homeland Security, CYBERCOM, Air Force Office of Special Investigations, and FBI who serve in the roles of NCIJTF Deputy Directors. This leadership team helps identify cross-agency gaps and redundancies that might otherwise hinder the NCIJTF's ability to develop, aggregate, integrate, and appropriately share information relating to the nation's most critical adversary-based cyber threats.

Central to its mission, the NCIJTF provides a means for multi-agency teams to address both standing and emerging issues related to cyber threat investigations across the federal, state, local, and international law enforcement, intelligence, counterintelligence, and military communities. For example, the NCIJTF develops and coordinates whole-of-government cyber campaigns, acting as the integrating mechanism among stakeholders and ensuring all pertinent community members are leveraged for maximum results.

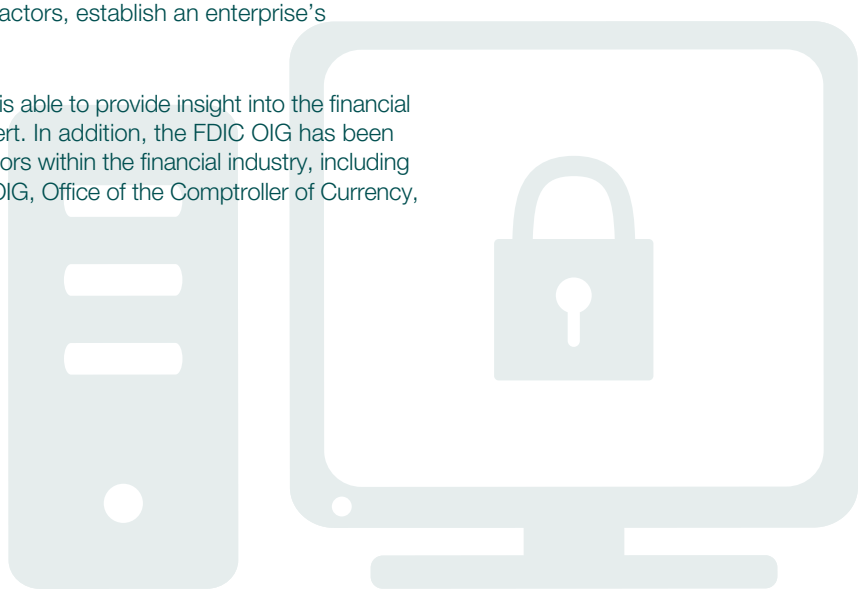
The NCIJTF collaborates closely with other Federal Cyber Centers, and as new cyber incidents arise, helps to ensure that the right U.S. government resources are brought to bear. The task force also provides guidance on financial investigative tools and techniques, generates new leads, and uncovers new cyber threats by exploiting financial data.

In addition, the NCIJTF continues to manage and evolve long-standing capabilities, such as its flexible and robust analytical platform that ingests and integrates increasing amounts of information from its partnering agencies. This provides a unique and holistic view of our nation's cyber threat and its vulnerabilities that the NCIJTF shares with cyber stakeholders. As the NCIJTF expands its platform and its capabilities, it helps to mature the analytical, investigative, and network defense capabilities of the U.S. government as well.

The NCIJTF collaborates directly with colleagues from a group of international U.S. partners. Representatives from Canada, Great Britain, Australia, and New Zealand work with NCIJTF assignees to identify mutual challenges and to develop common solutions in the cyber realm.

The OIG has assigned one of its special agents to the NCIJTF. Within the task force, the agent works within the Office of Threat Pursuit. This office supports U.S. government criminal and national security cyber operations and intelligence matters through case coordination, virtual currency consultation, and cyber-financial analysis. Specifically, the Office of Threat Pursuit enhances cyber investigations through the application of financial investigative techniques, procedures, and business acumen in order to identify evidence of criminal and national security threats, identify co-conspirators and benefactors, establish an enterprise's hierarchy, and identify and seize assets.

As a member of the NCIJTF, the FDIC OIG is able to provide insight into the financial industry by acting as a subject matter expert. In addition, the FDIC OIG has been able to coordinate with other federal regulators within the financial industry, including the Securities and Exchange Commission OIG, Office of the Comptroller of Currency, and others.



Dodd-Frank Act Risk Assessment and Related Work

Some months ago, the OIG undertook an initiative to keep current with the FDIC's efforts associated with implementation of risk management, monitoring, and resolution authorities emanating from the Dodd–Frank Act. Our purpose in doing so was to understand and analyze operational issues and emerging risks impacting the FDIC, the financial community, and internal OIG operations and plans. This continuous and focused risk assessment and monitoring was intended to enhance our more traditional, periodic OIG risk assessment and planning efforts and assist with the OIG's internal preparation efforts in the event a SIFI should fail. The assessment and monitoring provided an informal, efficient means of making FDIC and OIG management aware of issues and risks warranting attention.

We subsequently identified areas where we believed we could add value. To name a few, and as discussed earlier, we audited the FDIC's controls for safeguarding sensitive information in resolution plans, and we evaluated the FDIC's resolution plan review process. We have ongoing work related to the FDIC's monitoring of SIFIs and planned work to assess the FDIC's progress in establishing policies and procedures to receive funding to execute an orderly liquidation, its international coordination efforts to execute such a resolution, and its planned use of private sector resources to do so.

Additionally, under the Dodd-Frank Act—Title II Orderly Liquidation Authority, section 211, the FDIC IG shall conduct, supervise, and coordinate audits and investigations of the liquidation of any covered financial company by the Corporation as receiver under the title, including collecting and summarizing:

- a description of actions taken by the FDIC as receiver;
- a description of material sales, transfers, mergers, obligations, purchases, and other material transactions by the FDIC;
- an evaluation of the adequacy of the policies and procedures of the Corporation under section 203(d) and orderly liquidation plan under section 210(n)(14);
- an evaluation of the utilization by the FDIC of private sector in carrying out its function, including the adequacy of any conflict-of-interest reviews; and
- an evaluation of overall performance of the FDIC in liquidating the covered financial company, including administrative costs, timeliness of liquidation process, and impact on the financial system.

The timing of such work would be not later than 6 months after the date the Corporation is appointed receiver and every 6 months thereafter. Findings and evaluations are to be included in the IG's semiannual reports and the IG would appear before appropriate committees of the Congress, if requested.

The OIG views the above requirements to be highly significant to our office and the Corporation. We have planned for such an eventuality by researching issues relating to scope, frequency, reporting, funding, and needed resources. We are designating a project team to begin developing an audit approach to possible work and corresponding reporting mechanisms in line with Title II of the Act. We are also determining how best to capture and track any expenses we incur if we are statutorily required to audit or investigate any covered financial company by the Corporation as receiver. We will coordinate closely with corporate officials, as needed, in carrying out this work should the need arise.

Goal 5: Operational Efficiency and Workforce Excellence

Maximize OIG operational efficiency and workforce excellence

While the OIG's audit, evaluation, and investigation work is focused principally on the FDIC's programs and operations, we also hold ourselves to high standards of performance and conduct. We seek to recruit and retain a high-quality staff, and promote employee engagement at all levels of the organization. A major challenge for the OIG over the past few years was ensuring that we had the resources needed to effectively and efficiently carry out the OIG mission at the FDIC, given a sharp increase in the OIG's statutorily mandated work brought about by numerous financial institution failures, the FDIC's substantial resolution and receivership responsibilities, and its new resolution authorities under the Dodd-Frank Act. We now have a bit more discretion in planning our work and have been able to focus attention on certain corporate activities that we have not reviewed for some time. Still, however, we are facing future attrition in our OIG workforce and are currently operating below our authorized staffing level. As a result, we are closely monitoring our staffing and taking steps to ensure we are positioned to sustain quality work to address risk areas and replenish our human resources as OIG staff leave.

To ensure a high-quality staff, we must continuously invest in keeping staff knowledge and skills at a level equal to the work that needs to be done, and we emphasize and support training and development opportunities for all OIG staff. We also seek to ensure effective and efficient use of human, financial, IT, and procurement resources in conducting OIG audits, evaluations, investigations, and other support activities, and have a disciplined budget process to see to that end. In all of our operations, we want to leverage the capabilities of the technological tools at our disposal. That said, we are acutely aware of information security vulnerabilities and take steps to secure and safeguard the information that we possess.

Our office continues efforts to better manage the voluminous records in our possession—both in electronic and hard copy form. Records management activities are ongoing and designed to ensure the OIG maintains information needed to carry out its mission and respond to litigation needs or Congressional requests for documents. Similarly, we are seeking to more clearly capture and outline our policies and procedures for the numerous operational activities that we undertake on a daily basis to ensure that these activities occur efficiently and effectively.

To achieve excellence, the OIG must be professional, objective, fact-based, nonpartisan, fair, and balanced in all its work. Also, the IG and OIG staff must be free both in fact and in appearance from personal, external, and organizational impairments to their independence. As a member of CIGIE, the OIG is mindful of the *Quality Standards for Federal Offices of Inspector General*. Further, the OIG conducts its audit work in accordance with generally accepted government auditing standards; its evaluations in accordance with *Quality Standards for Inspection and Evaluation*; and its investigations, which often involve allegations of serious wrongdoing that may involve potential violations of criminal law, in accordance with *Quality Standards for Investigations* and procedures established by DOJ.

The OIG supports the Government Performance and Results Modernization Act of 2010, signed into law on January 4, 2011, and is committed to applying its principles of strategic planning and performance measurement and reporting to our operations. Importantly, the OIG has re-examined the strategic and performance goals and related activities that have guided our past efforts and revised them to provide the best framework within which to carry out our mission and achieve goals in the current FDIC and OIG operating environment.

OIG Work in Support of Goal 5

The following activities from the reporting period reflect our commitment to maximizing operational efficiency and ensuring workforce excellence:

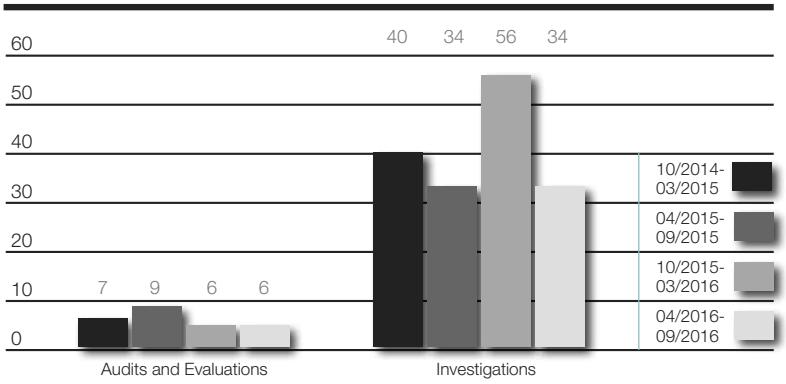
- Carried out longer-range OIG personnel and recruiting strategies to ensure a strong, effective complement of OIG resources going forward and in the interest of succession planning. Positions filled during the reporting period include a Deputy Assistant Inspector General for Investigations, Special Agent in Charge of the OIG's New York Regional Office, Special Advisor to the Acting IG, financial analysts, and auditors.
- Developed a program to recruit interns with skills in finance, IT, law, communications, and management, and planned for their involvement in ongoing OIG activities.
- Continued to support members of the OIG pursuing professional training and certifications or attending graduate banking school programs to enhance the OIG staff members' expertise and knowledge. OIG staff have been enrolled in the banking schools at Southwestern Graduate School of Banking, Southern Methodist University, Dallas; Graduate School of Banking, University of Wisconsin, Madison, Wisconsin; Colorado Graduate School of Banking, University of Colorado, Boulder, Colorado; and the American Bankers Association Commercial Lending School, Southwestern Methodist University, Dallas, Texas. Two OIG staff successfully completed their banking schools during the period.
- Researched options for a new training and development system to enable better tracking of professional development of OIG staff.
- Enrolled OIG staff in several different FDIC Leadership Development Programs to enhance their leadership capabilities.
- Hosted interns from the Federal Maritime Commission OIG for an information session to explain the role of the FDIC OIG and acquaint them with public service as they pursue possible career paths.
- Provided one of the members of the OIG's Counsel's Office to serve as a Special Assistant U.S. Attorney for multiple cases and trials involving bank fraud. This opportunity allows the Associate Counsel to apply legal skills as part of the prosecutorial teams in advance of and during the trials.
- Reviewed the OIG's performance management and awards programs to foster an understanding of their use and help ensure fairness and consistency in their application. Revised definitions of ratings to better convey performance expectations to all OIG staff.
- Implemented a new investigative case management system and worked to migrate audit and evaluation data and upgrade TeamMate.
- Continued efforts to update the OIG's records and information management program and practices to ensure an efficient and effective means of collecting, storing, and retrieving needed information and documents. Took steps to increase awareness of the importance of records management in the OIG, including through communications to OIG staff in headquarters and field locations.

- Undertook a number of initiatives to ensure security of the OIG's IT infrastructure and internal operations, including offering information sessions on Ransomware for OIG staff and disseminating IT security-related notifications to OIG staff.
- Addressed independence concerns regarding OIG to OIG internal emails residing in the FDIC's email vault and continued to coordinate with the Division of Information Technology as it remediates the problem of email comingling. Also hired a consultant to assist our office in independently reviewing how the problem was identified and is being remediated.
- Coordinated with a contractor to refine the technical and security requirements for redesign of the OIG's external Website.
- Reviewed and updated a number of OIG internal policies related to audit, evaluation, investigation, and management operations of the OIG to ensure they provide the basis for quality work that is carried out efficiently and effectively throughout the office and made substantial progress converting and transferring such policies to an automated policies and procedures repository for use by all OIG staff.
- Oversaw contracts to qualified firms to provide audit, evaluation, and other services to the OIG to provide support and enhance the quality of our work and the breadth of our expertise as we conduct audits, evaluations, and to complement other OIG functions and closely monitored contractor performance.
- Proposed and received the FDIC Chairman's approval of an FY 2018 budget of $39.1 million to fund 144 authorized positions, up 7 from FY 2017.
- Continued to monitor, track, and control OIG spending, particularly as it relates to OIG travel-related expenses, use of procurement cards, and petty cash expenditures.
- Relied on OIG Counsel's Office to provide legal advice and counsel to teams conducting audits and evaluations, and to support investigations of financial institution fraud and other criminal activity, in the interest of ensuring legal sufficiency and quality of all OIG work.
- Coordinated with the Railroad Retirement Board OIG as it conducted the peer review of the system of quality control for our audit organization.
- Undertook risk-based OIG planning efforts for audits, evaluations, and investigations for FY 2017 and beyond, taking into consideration the goals of, and risks to, FDIC corporate programs and operations and those risks more specific to the OIG. Devoted resources to developing a universe of FDIC programs, activities, and risk areas and used corporate performance goals as further input for identifying risk areas and priorities for OIG planned coverage. Incorporated such information in finalizing OIG strategic and performance plans.
- Finalized the OIG's Strategic Plan for 2017-2021, Performance Plan for FY 2017, and corresponding Audit and Evaluation Assignment Plan for the current fiscal year.

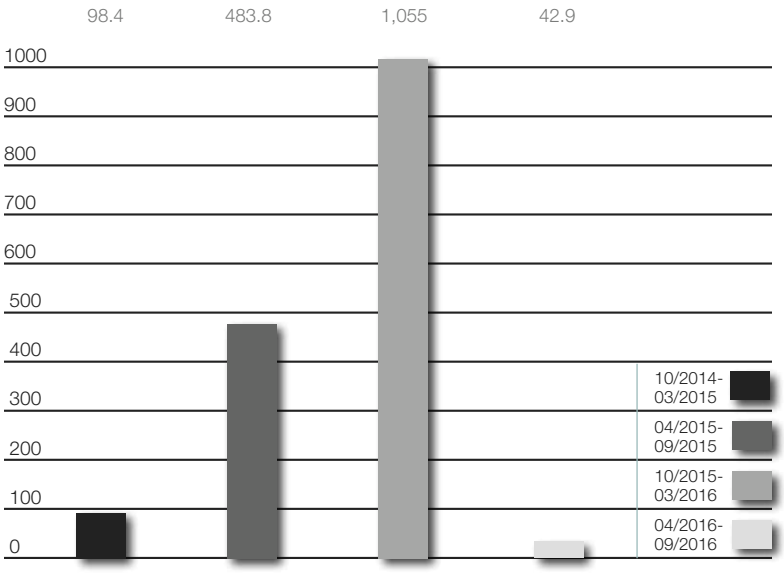
Cumulative Results (2-year period)

Nonmonetary Recommendations	
October 2014 – March 2015	35
April 2015 – September 2015	20
October 2015 – March 2016	12
April 2016 – September 2016	16

Products Issued and Investigations Closed



Fines, Restitution, and Monetary Recoveries Resulting from OIG Investigations ($ millions)



Reporting Requirements

Index of Reporting Requirements - Inspector General Act of 1978, as amended

Reporting Requirements	Page
Section 4(a)(2) Review of legislation and regulations	48
Section 5(a)(1) Significant problems, abuses, and deficiencies	10-34
Section 5(a)(2) Recommendations with respect to significant problems, abuses, and deficiencies	10-34
Section 5(a)(3) Recommendations described in previous semiannual reports on which corrective action has not been completed	49
Section 5(a)(4) Matters referred to prosecutive authorities	9
Section 5(a)(5) and 6(b)(2) Summary of instances where requested information was refused	53
Section 5(a)(6) Listing of audit reports	51
Section 5(a)(7) Summary of particularly significant reports	10-22
Section 5(a)(8): Statistical table showing the total number of audit reports and the total dollar value of questioned costs	52
Section 5(a)(9) Statistical table showing the total number of audit reports and the total dollar value of recommendations that funds be put to better use	52
Section 5(a)(10) Audit recommendations more than 6 months old for which no management decision has been made	53
Section 5(a)(11) Significant revised management decisions during the current reporting period	53
Section 5(a)(12) Significant management decisions with which the OIG disagreed	53

Evaluation report statistics are included in this report as well, in accordance with the Inspector General Reform Act of 2008.

Appendix 1

Information Required by the Inspector General Act of 1978, as Amended

Review of Legislation and Regulations

The FDIC OIG's review of legislation and regulations during the past 6-month period involved continuing efforts to monitor and/or comment on enacted law and/or proposed Congressional legislation, including the following:

- Public Law 114-94, Fixing America's Surface Transportation Act, (portions that address bank examination cycles, state regulation of financial service providers, and expansion of rural lending practices);
- H.R. 4781, the FDIC Accountability Act (no legislative action during the reporting period);
- H.R. 653, the FOIA Oversight and Implementation Act/S. 337, the FOIA Improvement Act (became Public Law 144-185);
- H.R. 4242, the Holding Individuals Accountable and Deterring Money Laundering Act (no legislative action during the reporting period);
- S. 579, the Inspector General Empowerment Act of 2015 (passed by Committee)/ H.R. 2395, the Inspector General Empowerment Act of 2016 (passed by the House of Representatives [House]);
- H.R. 2947, the Financial Institution Bankruptcy Act (passed by the House);
- H.R. 4359, the Administrative Leave Reform Act (passed by the House);
- S. 2133, the Fraud Reduction and Data Analytics Act (became Public Law 114-186); and
- Executive Order 13719, Establishment of the Federal Privacy Council (OMB issued implementing guidance on September 15, 2016).

Additionally, OIG Counsel's Office:

- Submitted to OMB comments on a draft version of an OMB Memorandum entitled, "Preparing for and Responding to a Breach of Personally Identifiable Information."
- Acted as a conduit between the OIG and the FDIC, specifically, the Legal Division, to obtain legal opinions and analyses on various topics of interest, including Executive Orders on classified information; and OMB publications on IT, privacy, and other matters.

Significant Recommendations from Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

This table shows the corrective actions management has agreed to implement but has not completed, along with any associated monetary amounts. In some cases, these corrective actions are different from the initial recommendations made in the audit or evaluation reports. However, the OIG has agreed that the planned actions meet the intent of the initial recommendations. The information in this table is based on (1) information supplied by FDIC's Corporate Management Control (CMC), Division of Finance and (2) the OIG's determination of closed recommendations. Recommendations are closed when (a) CMC notifies the OIG that corrective actions are complete or (b) in the case of recommendations that the OIG determines to be particularly significant, after the OIG confirms that corrective actions have been completed and are responsive. CMC has categorized the status of these recommendations as follows:

Management Action in Process:
(five recommendations from three reports)

Management is in the process of implementing the corrective action plan, which may include modifications to policies, procedures, systems, or controls; issues involving monetary collection; and settlement negotiations in process.

Table I: Significant Recommendations From Previous Semiannual Reports on Which Corrective Actions Have Not Been Completed

Report Number, Title & Date	Significant Recommendation Number	Brief Summary of Planned Corrective Actions and Associated Monetary Amounts
Management Action in Process		
AUD-14-002 **Independent Evaluation of FDIC's Information Security Program** November 21, 2013	**10**	Coordinate with the Division of Information Technology and FDIC division and office officials, as appropriate, to address potential gaps that may exist between the 12-hour timeframe required to restore mission essential functions following an emergency and the 72-hour recovery time objective for restoring mission-critical applications.
EVAL-15-003 **The FDIC's Supervisory Approach to Cyberattack Risks** March 18, 2015	**2**	Continue to work with members of the Federal Financial Institutions Examination Council to update the IT Handbook, including eliminating duplication and redundancy contained in the booklets.

Management Action in Process (continued)		
AUD-15-008 **FDIC's Role in Operation Choke Point and Supervisory Approach to Institutions that Conducted Business with Merchants Associated with High-Risk Activities** September 16, 2015	**1**	Review and clarify, as appropriate, existing policy and guidance pertaining to the provision and termination of banking services to ensure it adequately addresses banking products other than deposit accounts, such as credit products.
	2	Assess the effectiveness of the FDIC's supervisory policy and approach with respect to the issues and risks discussed in this report after a reasonable period of time is allowed for implementation.
	3	Review and clarify, as appropriate, existing supervisory policy and guidance to ensure it adequately defines moral suasion in terms of the types and circumstances under which it is used to address supervisory concerns, whether it is subject to sufficient scrutiny and oversight, and whether meaningful remedies exist should moral suasion be misused.

Table II: Audit and Evaluation Reports Issued by Subject Area

Audit/Evaluation Report		Questioned Costs		Funds Put to Better Use
Number and Date	**Title**	**Total**	**Unsupported**	
Supervision				
EVAL-16-006 September 28, 2016	*The FDIC's Resolution Plan Review Process*			
Receivership Management				
EVAL-16-005 June 30, 2016	*The FDIC's Controls Over Receivership Asset Securitizations*	$55,000		
AUD-16-003 July 6, 2016	*The FDIC's Controls for Mitigating the Risk of an Unauthorized Release of Sensitive Resolution Plans*			
Resources Management				
AUD-16-004 July 7, 2016	*The FDIC's Process for Identifying and Reporting Major Information Security Incidents*			
AUD-16-005 August 11, 2016	*The Cybersecurity Act of 2015 – The FDIC's Controls and Practices Related to Covered Systems*			
AUD-16-006 September 23, 2016	*The FDIC's Preparedness Efforts to Implement the Requirements of the DATA Act*			
Totals for the Period		**$55,000**	**$0**	**$0**

Table III: Audit and Evaluation Reports Issued with Questioned Costs

		Questioned Costs	
	Number	Total	Unsupported
A. For which no management decision has been made by the commencement of the reporting period.	0	$0	$0
B. Which were issued during the reporting period.	1	$55,000	$0
Subtotals of A & B	**1**	**$55,000**	**$0**
C. For which a management decision was made during the reporting period.	0	$0	$0
(i) dollar value of disallowed costs.	1	$55,000	$0
(ii) dollar value of costs not disallowed.	0	$0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0	$0

Table IV: Audit and Evaluation Reports Issued with Recommendations for Better Use of Funds

	Number	Dollar Value
A. For which no management decision has been made by the commencement of the reporting period.	0	$0
B. Which were issued during the reporting period.	0	$0
Subtotals of A & B	**0**	**$0**
C. For which a management decision was made during the reporting period.	0	$0
(i) dollar value of recommendations that were agreed to by management.	0	$0
- based on proposed management action.	0	$0
- based on proposed legislative action.	0	$0
(ii) dollar value of recommendations that were not agreed to by management.	0	$0
D. For which no management decision has been made by the end of the reporting period.	0	$0
Reports for which no management decision was made within 6 months of issuance.	0	$0

Table V: Status of OIG Recommendations Without Management Decisions

During this reporting period, there were no recommendations more than 6 months old without management decisions.

Table VI: Significant Revised Management Decisions

During this reporting period, there were no significant revised management decisions.

Table VII: Significant Management Decisions with Which the OIG Disagreed

During this reporting period, there were no significant management decisions with which the OIG disagreed.

Table VIII: Instances Where Information Was Refused

During this reporting period, there were no instances where information was refused.

Appendix 2

Information on Failure Review Activity (required by the Dodd-Frank Wall Street Reform and Consumer Protection Act)

FDIC OIG Review Activity for the Period April 1, 2016 through September 30, 2016
(for failures that occur on or after January 1, 2014 causing losses to the DIF of less than $50 million)

Institution Name	Closing Date	Estimated Loss to DIF (Dollars in Millions)	Grounds Identified by the State Bank Supervisor for Appointing the FDIC as Receiver	Unusual Circumstances Warranting In-depth Review?
Reviews Completed				
North Milwaukee State Bank (Milwaukee, Wisconsin)	3/11/16	$9.6	The bank exhibited extremely unsafe and unsound practices and conditions.	No
Reviews Ongoing				
The Woodbury Banking Company (Woodbury, Georgia)	8/19/16	$5.2		
First CornerStone Bank (King of Prussia, Pennsylvania)	5/6/16	$10.8		
Trust Company Bank (Memphis, Tennessee)	4/29/16	$7.2		

Appendix 3

Peer Review Activity (required by the Dodd-Frank Wall Street Reform and Consumer Protection Act)

Section 989C of the Dodd-Frank Act contains additional semiannual reporting requirements pertaining to peer review reports. Federal Inspectors General are required to engage in peer review processes related to both their audit and investigative operations. In keeping with section 989C, the FDIC OIG is reporting the following information related to its peer review activities. These activities cover our most recent roles as both the reviewed and the reviewing OIG and relate to both audit and investigative peer reviews.

Audit Peer Reviews

On the audit side, on a 3-year cycle, peer reviews are conducted of an OIG audit organization's system of quality control in accordance with the CIGIE *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*, based on requirements in the *Government Auditing Standards* (Yellow Book). Federal audit organizations can receive a rating of pass, pass with deficiencies, or fail.

- The U.S. Department of State (DOS) and the Broadcasting Board of Governors OIG conducted a peer review of the FDIC OIG's audit organization and issued its system review report on September 17, 2013. In the DOS OIG's opinion, the system of quality control for our audit organization in effect during the period April 1, 2011 through March 31, 2013, had been suitably designed and complied with to provide our office with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. We received a peer review rating of pass.

The report's accompanying letter of comment contained six recommendations that, while not affecting the overall opinion, were designed to further strengthen the system of quality control in the FDIC OIG Office of Audits and Evaluations.

As of September 30, 2014, we considered all recommendations to be closed.

This peer review report (the system review report and accompanying letter of comment) is posted on our Web site at www.fdicig.gov

Our Office of Audits and Evaluations has been peer reviewed by the Railroad Retirement Board OIG. Results of that review will be included in our next semiannual report. We have also begun a peer review of the audit organization of the Tennessee Valley Authority OIG.

Definition of Audit Peer Review Ratings

Pass: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

Pass with Deficiencies: The system of quality control for the audit organization has been suitably designed and complied with to provide the OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects with the exception of a certain deficiency or deficiencies that are described in the report.

Fail: The review team has identified significant deficiencies and concludes that the system of quality control for the audit organization is not suitably designed to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects or the audit organization has not complied with its system of quality control to provide the reviewed OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects.

FDIC OIG Peer Review of the National Archives and Records Administration OIG

The FDIC OIG completed a peer review of the audit operations of the National Archives and Records Administration (NARA) OIG, and we issued our final report to that OIG on April 30, 2014. We reported that in our opinion, the system of quality control for the audit organization of the NARA OIG, in effect for the 12 months ended September 30, 2013, had been suitably designed and complied with to provide the NARA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards in all material respects. The NARA OIG received a peer review rating of pass.

As is customary, we also issued a Letter of Comment, dated April 30, 2014, that set forth findings and recommendations that were not considered to be of sufficient significance to affect our opinion expressed in the system review report. We made 14 recommendations. In updating the status of those recommendations for this reporting period, NARA OIG informed us that it had fully implemented all recommendations as of October 1, 2016. NARA OIG posted the peer review report (system review report) on its Web site at www.archives.gov/oig/.

Investigative Peer Reviews

Quality assessment peer reviews of investigative operations are conducted on a 3-year cycle as well. Such reviews result in a determination that an organization is "in compliance" or "not in compliance" with relevant standards. These standards are based on *Quality Standards for Investigations* and applicable Attorney General Guidelines. For our office, applicable Attorney General Guidelines include the *Attorney General Guidelines for Offices of Inspectors General with Statutory Law Enforcement Authority* (2003), *Attorney General Guidelines for Domestic Federal Bureau of Investigation Operations* (2008), and *Attorney General Guidelines Regarding the Use of Confidential Informants* (2002).

- The Department of the Treasury OIG conducted the most recent peer review of our investigative function and issued its final report on the quality assessment review of the investigative operations of the FDIC OIG on February 1, 2016. The Department of the Treasury OIG reported that in its opinion, the system of internal safeguards and management procedures for the investigative function of the FDIC OIG in effect for the year ending December 31, 2015, was in compliance with quality standards established by CIGIE and applicable Attorney General guidelines. These safeguards and procedures provided reasonable assurance of conforming with professional standards in the planning, execution, and reporting of FDIC OIG investigations.

- The FDIC OIG conducted a peer review of the investigative function of the Environmental Protection Agency (EPA) OIG. We issued our final report to EPA OIG on December 2, 2014. We reported that, in our opinion, the system of internal safeguards and management procedures for the investigative function of the EPA OIG in effect for the period October 1, 2012 through September 30, 2013 was in compliance with the quality standards established by CIGIE and Attorney General Guidelines.

Congratulations and Farewell

Congratulations and farewell to members of the FDIC OIG who have recently retired:

Leslee Bollea

Leslee A. Bollea retired after 36 years of federal service. She began her career as a summer intern at the U.S. Department of Defense, Washington headquarters, and in June 1980 joined the U.S. General Accounting Office (GAO) (now the Government Accountability Office) as a management analyst. Leslee joined the OIG at the Resolution Trust Corporation (RTC) in October 1990, where she made significant contributions as a member of the Office of Congressional Relations and Management. Upon the RTC's sunset in December 1995, she joined the FDIC OIG's Office of Management.

While at the FDIC OIG, Leslee supported IG Gaston L. Gianni, Jr., in his role as Vice Chair of the President's Council on Integrity and Efficiency (PCIE), and in that capacity, joined colleagues in the Executive Council on Integrity and Efficiency (ECIE) to provide invaluable support to the federal IG community in the interest of ensuring economy, efficiency, effectiveness, and integrity government-wide. She continued her active involvement in the successor organization to the PCIE and ECIE—the Council of the Inspectors General on Integrity and Efficiency (CIGIE), particularly through her support of FDIC IG Jon T. Rymer during his entire tenure as CIGIE Audit Committee Chair.

In August 2009, Leslee transferred to the IG's Immediate Office and assumed the role of Senior Congressional Relations Manager in August 2010. As the individual responsible for the OIG's Congressional Relations activities, she developed Congressional protocols, forged strong working relationships with the Committee staff of Members of the U.S. Senate and House of Representatives, coordinated with the FDIC's Office of Legislative Affairs, and monitored and advised the IG and OIG staff on matters of Congressional interest.

In December 2014, Leslee was detailed to the Department of Defense OIG to assist the Lead Inspector General for *Operation Inherent Resolve*—designated on October 17, 2014 by the Secretary of Defense as a contingency operation to defeat the Islamic State of Iraq and the Levant and deny them safe haven. Upon her retirement from the FDIC OIG in April 2016, she resumed work at the Department of Defense in this same capacity.

Alina Russell

Alina Russell began her career as a clerk typist with the Corporation's Division of Liquidation in Oklahoma City, Oklahoma, in April 1985. In July 1986, she took on additional responsibilities in that office as a liquidation technician and eventually assumed the role of secretary in May 1989. In October 1993, her duty station changed to the FDIC's consolidated office in Addison, Texas, and for the next several years, she worked for the Division of Liquidation, the Division of Depositor and Asset Services, and the Division of Finance at that location. In September 1986, Alina joined the FDIC OIG in the Dallas Regional Office as a secretary and subsequently became an investigative assistant—a position she held up to her retirement.

Over the past 20 years, Alina provided dedicated assistance to four Special Agents in Charge in Dallas and also served the Special Agents in Charge in the OIG's Kansas City, Chicago, and San Francisco regional offices. Her expertise in database searches and coordination with headquarters on important investigative and administrative matters also facilitated OI efforts nationwide.

Joe Seitz

Joe Seitz retired after nearly 14 years of federal service. His federal career began in June 1967, when he worked as a National Bank Examiner for the Office of the Comptroller of the Currency (OCC) in Minneapolis, Minnesota. Shortly thereafter, he was on military furlough and served in the U.S. Army from July 1967 to July 1969, which included a tour in Vietnam, where he received the Purple Heart as a result of wounds received in combat.

Following his safe return home, Joe rejoined the OCC in Minneapolis, and for the next 5 years, advanced steadily in his career as a National Bank Examiner. In July 2009, following many years working in the private sector banking arena, Joe joined the FDIC OIG where, for the past 7 years, he was a senior banking advisor, sharing his wealth of banking knowledge with his colleagues.

Joe played a key role with respect to the OIG's countless material loss reviews, where his insights in addressing the adequacy of bank management's risk management practices were invaluable. Equally, his contributions to our work involving commercial real estate and acquisition, development, and construction concentration risks and the FDIC's supervisory approach to cybersecurity risks were highly significant.

Howard Trebelhorn

Howard Trebelhorn retired after more than 37 years of federal service. His federal career began in 1975 when he worked as an accountant trainee with the Naval Audit Service in the Department of the Navy in Camden, New Jersey. While at the Department of the Navy, he advanced as an accountant and was later promoted to an auditor position. In 1984, he moved on to become an auditor at the Naval Audit Service, Department of the Navy, in Arlington, Virginia.

In 1987, Howard transferred to the Federal Home Loan Bank Board OIG, where he worked as an auditor until October 1989. During his time there, he earned the title of Certified Public Accountant from the State of Pennsylvania. Following the merger of the Bank Board with the FDIC in October 1989, Howard transferred to the FDIC OIG's Washington D.C. office as an auditor, and during his tenure in the OIG, he served as an auditor, audit specialist, and program analyst.

Howard contributed to the OIG's internal quality control reviews to help ensure the FDIC OIG's adherence to government auditing standards and internal OIG policies and procedures. He also assisted in conducting external peer reviews of other federal audit agencies under the IG community's peer review program. He coordinated numerous FDIC OIG assurance statements, attesting to the Chairman that the FDIC OIG's management control systems provide reasonable assurance that internal control requirements of key federal guidelines and regulations had been met. He also coordinated office-wide reviews of FDIC policies, interacted with FDIC facilities staff, and handled the OIG's emergency preparedness activities to ensure the safety and security of his OIG colleagues.

In Memoriam

In Memoriam

The OIG lost a great friend and former colleague recently when former Resolution Trust Corporation (RTC) IG, Jack Adair, passed away on July 15, 2016. Jack had served as the RTC IG from 1989 through the RTC's sunset on December 31, 1995.

Jack had an outstanding career at the General Accounting Office prior to his appointment as the RTC IG. He led the RTC OIG through a very complex time and contributed greatly to the RTC's successes in the resolution of the savings and loan crisis. The organization he built became an integral part of the FDIC OIG following the merger of RTC back into the FDIC. Subsequent to his retirement from the RTC, Jack became the Auditor to the Board of Supervisors, Fairfax County, Virginia, a position he held for more than 12 years before his ultimate retirement.

Those of us who had the good fortune to work for Jack will always remember his warm personality and sense of humor, but even more the dignity he always displayed however tough times became. Jack was a superb leader and a key figure in the history of our office as well as the Inspector General community as a whole.

Federal Deposit Insurance Corporation
Office of Inspector General
3501 Fairfax Drive
Arlington, VA 22226

To learn more about the FDIC OIG and for more information on matters discussed in this Semiannual Report, visit our Website: http://www.fdicig.gov

The Office of Inspector General (OIG) Hotline is a convenient mechanism employees, contractors, and others can use to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations. The OIG maintains a toll-free, nationwide Hotline **(1-800-964-FDIC)**, electronic mail address **(IGhotline@FDIC.gov)**, and postal mailing address. The Hotline is designed to make it easy for employees and contractors to join with the OIG in its efforts to prevent fraud, waste, abuse, and mismanagement that could threaten the success of FDIC programs or operations.

DESIGN: FDIC/DOA/CSB/GRAPHIC DESIGN AND PRINTING UNIT