Budget for Fiscal Year 2019

February 2018

Table of Contents

Office of Inspector General
Budget for Fiscal Year 2019

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) presents its proposed budget for Fiscal Year (FY) 2019. In this document, we will present the following information:

- Mission and Vision
- Source of OIG Funding
- Proposed Fiscal Year 2019 Budget
- OIG Accomplishments in 2017
    - Audit and Evaluation Reports
    - Results of OIG Investigations
- Top Challenges Facing the FDIC and Focus for Future OIG Work

MISSION AND VISION

The Congress created the FDIC in 1933 to restore public confidence in the nation's banking system. The FDIC insures more than $7 trillion in deposits at more than 5,700 banks and savings associations and directly supervises about 3,700 of these banks. It promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The FDIC receives no Congressional appropriations - it is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and from earnings on investments in U.S. Treasury securities.

The FDIC OIG is an independent organization established under the Inspector General Act of 1978, as amended. The FDIC OIG mission is to prevent, deter, and detect fraud, waste, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency. In carrying out this mission, the OIG

- Conducts audits, evaluations, and investigations;
- Reviews existing and proposed legislation and regulations; and
- Keeps the FDIC Chairman and the Congress informed of problems and deficiencies relating to FDIC programs and operations.

The vision for the Office is to serve the American people as a recognized leader in the Inspector General community: driving change and making a difference by prompting and encouraging improvements and efficiencies at the FDIC; and helping to preserve the integrity of the agency and the banking system, and protect depositors and financial consumers.

The OIG fully supports and participates in IG community activities through the Council of the Inspectors General on Integrity and Efficiency. We also coordinate closely with representatives from the other financial regulatory OIGs. In this regard, the Dodd-Frank Wall Street Reform and Consumer Protection

Act (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 Inspector General as it relates to the broader financial sector and ways to improve financial oversight.

In addition, we meet with representatives of the Government Accountability Office to coordinate work efforts. We also partner with representatives of the Department of Justice, including the Federal Bureau of Investigation and U.S. Attorneys' Offices, and with other OIGs to coordinate our criminal investigative work.

The FDIC OIG also has a statutory responsibility to review each failed FDIC-supervised institution. In instances where the loss to the FDIC's Deposit Insurance Fund (DIF) is greater than $50 million, the OIG is required to conduct a Material Loss Review to determine the causes of failure and evaluate the FDIC's supervision of the institution. The OIG also conducts a review of the FDIC's information security program and practices pursuant to the Federal Information Security Modernization Act of 2014 (FISMA).

Appendix I presents an overview of the OIG's current organizational structure and a brief description of our component divisions. Appendix II presents a brief summary of the OIG's accomplishments in FY 2017.

SOURCE OF OIG FUNDING

The FDIC OIG receives a specific appropriation. The funding source for the FDIC OIG, and the FDIC, is the Deposit Insurance Fund (DIF), not the U.S. Treasury. The DIF is funded by assessments paid by insured banks and thrifts based on an institution's average assets less average tangible equity, and from interest on the required investment of fund reserves held in government securities. The funding level for the OIG is set by appropriation in accordance with Section 1105(a) of Title 31, United States Code, which provides separate appropriations accounts for Offices of Inspector General in order to preserve their budgetary independence from the parent agency. The funding level for the OIG is incorporated into the FDIC's budget, with funding allocated to the OIG from the DIF.

PROPOSED FISCAL YEAR 2019 BUDGET

The OIG's proposed FY 2019 budget is $43 million. Of this amount, approximately $37 million (86 percent) is allocated to personnel costs, including benefits. The remaining $6 million (14 percent) includes information technology (IT) expenditures, travel costs, contract-related expenses, and contributions to the Council of Inspectors General on Integrity and Efficiency. The budget supports an authorized staffing level of 144, reflecting no change from FY 2018.

We are requesting an increase in our budget of $2.9 million for upgrades and improvements to our IT systems and processes. Most of this funding ($2 million) will be devoted to our Electronic Crimes Unit (ECU), which conducts cyber forensic analysis for our criminal investigations. ECU's support has become a mission-critical function within the OIG's investigative operations, and its capabilities significantly

strengthen our investigations. ECU collects and preserves evidence in electronic form through forensic imaging; this evidence is then used to investigate matters and at trials. Since 2012, the ECU has assisted agents on investigations resulting in more than 180 convictions, $3.8 billion in court-ordered restitution, and nearly $65 million in forfeited assets. ECU is currently engaged in more than 40 open OIG-led criminal investigations, or almost 25 percent of all open OI investigations, and it is conducting an additional 12 cyber- or computer-related investigations. We anticipate growth in the ECU with the continued integration of electronic equipment and data within banking and commercial activities. The funding for ECU will be used to enhance the storage capacity, backup, security, and disaster recovery capabilities. We will allocate the remaining IT funds to upgrade our aging internal IT infrastructure and maintain the functionality and security of our systems.

While not directly or immediately impacting our budget, the OIG will be moving its e-mail to the Cloud. This transition will require substantial effort on the part of our office's IT staff and collaboration with the FDIC and its contractors. Further, consistent with federal "Cloud First" policy, the FDIC will evaluate safe, secure cloud computing options before making any new IT investments. That strategy presents uncertainties and challenges for our office. Specifically, if Cloud-related initiatives result in requirements unique to the OIG, they could impact our budget and staffing in FY 2019 and future fiscal years. Recognizing that these IT operational issues have become integral to accomplishing our mission and that we must maintain our systems securely and efficiently, we recently established a new Office of Information Technology that will report directly to our Principal Deputy Inspector General.

Appendix III presents our OIG Budget Request for FY 2019.

OIG ACCOMPLISHMENTS IN 2017

Addressing cybersecurity risks in the financial sector and safeguarding its own computer systems and data is a top FDIC priority. To enhance our focus in this area, we reorganized the OIG's audit and evaluation function. We created a new Office of IT Audits and Cyber (ITC) and a separate Office of Program Audits and Evaluations (PAE). The ITC office conducts audits of IT risks and challenges, both external to banks and the financial sector and internal to the FDIC's own systems. The FDIC also carries out diverse and important programs in accomplishing its mission and goals. In that regard, the PAE office conducts program evaluations and performance audits to assess the effectiveness of FDIC operations, compliance matters, and other systemic issues. We also revamped how we follow up on our audit and evaluation recommendations to ensure that the FDIC implemented OIG recommendations in a timely and effective manner.

We also undertook several initiatives to improve the efficiency and effectiveness of our office. We launched a new external website that is easier to use for Congressional staff and the public, and we are now uploading our reports to the new CIGIE website on www.oversight.gov, which provides a central repository for all public IG reports. Moreover, to increase transparency, we launched our Twitter account to post Tweets about our OIG public reports, cases, work activities, and other announcements, and convey relevant information about our accomplishments.

The OIG also re-energized its Whistleblower Ombudsperson program in accordance with the Whistleblower Protection Enhancement Act. Our Office was certified by the Office of Special Counsel (OSC) under its Certification Program, pursuant to 5 U.S.C. Section 2302(c). The FDIC OIG's completion of OSC's certification program demonstrates our commitment to whistleblowers and the remedies available under federal law. In addition, the FDIC OIG worked with the FDIC to reinforce such protections through training and awareness programs.

AUDIT AND EVALUATION REPORTS

During 2017, we issued 13 audit and evaluation reports, made 63 recommendations to strengthen controls in FDIC programs and operations, and identified questioned costs of $126,593. Our work covered diverse topics such as information security, the FDIC's response to data breaches, controls over separating employees' access to sensitive information, technology service provider contracts with financial institutions, monitoring of Systemically Important Financial Institutions, a material loss review of a failed financial institution, the FDIC efforts to ensure shared loss agreement recoveries are remitted, the FDIC's contracts related to managing failed bank data as receiver for failed institutions, and the FDIC's Work-in-Place program and hiring processes.

The following discussion highlights the findings from certain recently completed FDIC OIG audit and evaluation assignments.

The FDIC's Identity, Credential, and Access Management (ICAM) Program

The FDIC established the ICAM program in February 2011 to address the goals and objectives of Homeland Security Presidential Directive (HSPD)-12, *Policy for a Common Identification Standard for Federal Employees and Contractors*. HSPD-12 requires (among other things) that executive departments and agencies implement a government-wide standard for secure and reliable forms of credentials for eligible employees and contractor personnel to access federally-controlled facilities and information systems.

Our audit from September 2015 found that like other agencies, the FDIC had been confronted with technical hurdles and challenges in implementing its ICAM program. We found that despite the relatively significant investment in corporate resources involved, the ICAM program was not subject to sufficient and consistently robust governance, which resulted in limited success. The report contained two recommendations for the FDIC to (1) define the goals and approach for implementing the ICAM program, and (2) establish appropriate governance measures over the ICAM program.

In 2017, we issued a follow-up report on the ICAM program, and we found that the Corporation had taken corrective actions that were sufficient for us to close the recommendations in our September 2015 ICAM Audit Report. However, there were risks warranting management's attention as the Corporation issued Personal Identity Verification (PIV) cards to its employees and contractor personnel and enabled the cards to support access to the corporate network. Our report also noted that the FDIC had not established policies and procedures governing the management and use of PIV cards for physical and logical access and did not maintain current, accurate, and complete contractor personnel

data needed to manage PIV cards. Three of the four recommendations associated with these issues have been implemented to date.

Access to Sensitive Information by Employees Leaving the FDIC

The FDIC experienced a number of data breaches in late 2015 and early 2016 that involved employees who were exiting the FDIC. Between February and May 2016, the FDIC notified the Congress of seven major incidents in which departing employees inappropriately took significant quantities of sensitive information. The information taken was associated with financial institutions and their customers, creating the risk of unauthorized disclosure. The FDIC OIG examined issues related to the FDIC's policies governing departing employees' access to sensitive financial information. We reviewed procedures for separating FDIC employees and FDIC contractors.

We reported that, as designed, the program controls did not provide reasonable assurance that the pre-exit clearance process would identify unauthorized access to, or inappropriate removal and disclosure of, sensitive information in a timely or effective manner. Weaknesses existed in the design of certain controls; Divisions were not always following procedures; and the FDIC needed to strengthen its pre-exit clearance process. We further concluded that separating contractors may present greater risks than separating FDIC employees. We found several differences between the pre-exit clearance process for FDIC employees and contractors that increase risks related to protecting sensitive information when contractors separate.

To strengthen its process, the FDIC needed to ensure consistency between employee and contractor pre-exit clearance processes, reiterate responsibilities and expectations for oversight managers and records liaisons, and require timely notice of separating contractors. We made 11 recommendations to address the weaknesses we identified. The FDIC concurred with the recommendations.

Responding to Breaches of Personally Identifiable Information (PII)

We conducted an audit to assess the adequacy of the FDIC's processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and notifying and providing services to those individuals, when appropriate.

We reported that the FDIC had established formal processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and providing notification and services to those individuals, when appropriate. However, the implementation of these processes was not adequate. Specifically, the FDIC did not complete key breach investigation activities and notify affected individuals timely; did not adequately document key assessments and decisions; and needed to strengthen controls over its data breach management team, the group primarily responsible for handling breaches of PII. Additionally, the FDIC did not track and report key breach response metrics to benchmark and continuously improve its breach prevention and response capabilities.

We made seven recommendations to address the issues we identified. The FDIC concurred with the recommendations.

FISMA Audit—2017

Our review found security control weaknesses that limited the effectiveness of the FDIC's information security program and practices, and placed the confidentiality, integrity, and availability of the FDIC's information systems and data at risk.

Our report contained 19 findings, the most significant of which were:

- **Contingency Planning**. The FDIC's IT restoration capabilities were limited, and the agency had not taken timely action to address known limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster. Therefore, the FDIC could not be sure that it could maintain or restore its mission essential functions during an emergency within applicable timeframes.
- **Information Security Risk Management**. The FDIC established the Information Security Risk Advisory Council in 2015. However, the Council did not fulfill several of its key responsibilities as defined in FDIC policy.
- **Enterprise Security Architecture**. The FDIC had not established an enterprise security architecture, which increased the risk that the FDIC's information systems would be developed with inconsistent security controls that would be costly to maintain.
- **Technology Obsolescence**. The FDIC was using certain software in its server operating environment that was at the end of its useful life and for which the vendor was not providing support to the FDIC, thus allowing the potential for adversaries to exploit new weaknesses.
- **Information Security Strategic Plan.** The FDIC had drafted, but not yet finalized, an information security strategic plan.
- **Patch Management.** We noted instances in which patches addressing high-risk vulnerabilities were not installed on servers, desktop computers, and laptop computers within the timeframes established by FDIC policy.
- **Credentialed Scanning.** We found instances in which network IT devices were not subject to a "credentialed" scan—a thorough type of scan that involves logging into the IT device to inspect for vulnerabilities.
- **Security Information and Event Management (SIEM) Tool.** The FDIC had not developed a process to ensure that all servers on the FDIC's network route log data to the FDIC's SIEM tool.

We made 18 recommendations to improve the effectiveness of the FDIC's information security program controls and practices. FDIC management concurred with all recommendations. We determined that, according to the FISMA Reporting Metrics, the FDIC was rated as "Defined," which indicated that policies and procedures were formalized and documented, but not consistently implemented.

IT Hardware Asset Management

The FDIC uses IT hardware assets, among other things, for personal computing throughout the FDIC, supporting network operations, and providing communications connectivity. At the time of our fieldwork, the FDIC had 38,796 IT hardware items in inventory, including laptops, workstations, desktops, tablets, printers, scanners, servers, drives, routers, mainframes, and other equipment. IT

hardware assets are vulnerable to several risks, including inefficient or costly procurement, delays in deployment, equipment theft and obsolescence, and data loss. We evaluated the FDIC's controls over its IT Hardware Asset Management Program.

We reported that the FDIC had established some key controls over the IT hardware asset management program, including policies and procedures that specified roles and responsibilities for employees and contractors. However, we found that the FDIC needed to update its policies and procedures and strengthen its controls in most aspects of the program. Further, data needed to manage the program was frequently unreliable. Collectively, these weaknesses created an environment in which the FDIC was vulnerable to ineffectively managing IT hardware assets or having them lost or stolen.

We made nine recommendations for the FDIC to enhance asset management life cycle policies and procedures to reflect current practices; strengthen controls to better ensure program objectives are met; and improve the IT asset management tracking system data entry, reliability, and reporting to support IT asset management and decision-making. The FDIC concurred with our recommendations.

Material Loss Review—First NBC Bank, New Orleans, Louisiana

We issued a Material Loss Review of the Failure of First NBC Bank (First NBC), New Orleans, Louisiana, in which we analyzed the causes of First NBC's failure and evaluated the FDIC's supervision of the bank. The Louisiana Office of Financial Institutions (OFI) closed First NBC and appointed the FDIC as Receiver on April 28, 2017. First NBC's total assets at closing were $4 billion, and the estimated loss to the Deposit Insurance Fund was about $997 million.

We reported that with respect to the causes of failure, First NBC exhibited many of the characteristics of bank failures that we have identified in prior Material Loss Reviews and other reviews of the FDIC's supervision program, for example:

- a dominant official with broad lending authority and limited Board of Directors oversight,
- rapid growth funded by high-cost deposits, and
- large lending relationships and concentrations without adequate risk management controls to mitigate the risks.

The bank also developed significant concentrations in trade receivables and complex tax credit investments. The losses the bank realized on its large loan relationships, trade receivables, and tax credit investments severely diminished earnings and depleted capital to a point at which the bank could not recover.

As for the FDIC's supervision of First NBC, between 2006 and 2017, the FDIC and OFI conducted nine full scope joint safety and soundness examinations and six visitations of First NBC consistent with requirements. However, the FDIC's use of enforcement actions and examination ratings to address First NBC's issues was counter to the agency's forward-looking supervisory approach. That is, although examiners identified repeated risk management weaknesses, they relied too heavily on the bank's

financial condition and ability to raise capital in taking supervisory action and assigning management and asset quality ratings.

We made two recommendations in this report and management concurred.

RESULTS OF OIG INVESTIGATIONS

The OIG's Office of Investigations conducts its work to prevent, detect, and investigate criminal or otherwise prohibited activity that may harm or threaten to harm the operations or integrity of the FDIC and its programs. 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 Deposit Insurance Fund. Real estate developers and agents, attorneys, accountants, and other individuals involved in residential and commercial lending activities have also been implicated in a number of our cases. Other investigations have involved entities failing to maintain effective anti-money laundering programs or to file suspicious activity reports (SAR) with the Financial Crimes Enforcement Network following a suspected incident of money laundering or fraud, as required by the Bank Secrecy Act (BSA). When found guilty, the subjects of our investigations are held accountable through prison sentences and restitution, and other monetary penalties ordered.

During FY 2017, FDIC OIG investigations resulted in 122 indictments/informations; 101 convictions; 40 arrests; and fines, restitution, asset forfeitures and civil recoveries exceeding $231 million. The following cases are illustrative of those OIG investigative accomplishments, achieved through collaborative efforts with the Department of Justice, other OIGs, and federal, state, and local law enforcement entities.

Former Global Head of HSBC's Foreign Exchange Cash-Trading Found Guilty of Orchestrating Multimillion-Dollar Front-Running Scheme

On October 23, 2017, the former head of global foreign exchange (FX) cash trading at HSBC Bank plc was convicted at trial of one count of conspiracy to commit wire fraud and eight counts of wire fraud for his role in defrauding two bank clients through a multi-million dollar front-running scheme.

HSBC was selected to execute an FX transaction related to a planned sale of one of a client's foreign subsidiaries, which would require converting approximately $3.5 billion in sales proceeds into British Pounds Sterling. HSBC's agreement with the client required the bank to keep the details of the planned transaction confidential.

Instead, the former bank executive and other traders acting under the former bank executive's direction purchased Pounds Sterling for their own benefit in their HSBC proprietary accounts. The former bank executive then caused the $3.5 billion foreign exchange transaction to be executed in a manner that was designed to drive up the price of the Pounds Sterling, generating $7.3 million in profits for their proprietary positions and HSBC at the expense of their client.

HSBC Holdings plc, the parent company of HSBC Bank plc, also recently entered into a deferred prosecution agreement and agreed to pay a $63.1 million criminal penalty and $38.4 million in disgorgement and restitution to resolve charges related to this and a second, similar front-running scheme.

Former CEO and Former Chief Loan Officer of Failed Sonoma Valley Bank Convicted of Bank Fraud

On December 18, 2017, the former Chief Executive Officer and former Chief Loan Officer of the failed Sonoma Valley Bank were convicted at trial of conspiracy, bank fraud, money laundering, falsifying bank records, lying to bank regulators, and other crimes. An attorney for a real estate developer (who had been indicted on these charges before his death) was also convicted of conspiracy, bank fraud, attempted obstruction of justice, and other offenses.

Between 2004 and 2010, Sonoma Valley Bank loaned the developer and the people and entities he controlled in excess of $35 million, nearly $25 million more than the legal lending limit set by the bank's regulators. To conceal this high concentration of lending, the former CEO and Chief Loan Officer recommended that the bank approve multi-million dollar loans to straw borrowers. The former Chief Loan Officer was also convicted of taking a $50,000 bribe from the developer for some of the loans made to the straw borrowers.

The former CEO and Chief Loan Officer also conspired with the developer's attorney to mislead Sonoma Valley Bank into lending millions more to the developer, again in the name of a straw borrower, so the developer could illegally buy back, at a steep discount, a debt he owed to IndyMac Bank, which had failed and been taken over by the FDIC. FDIC rules specifically prohibited delinquent borrowers, like the developer, from purchasing their own notes at auction.

The former CEO and Chief Loan Officer were convicted of making false statements to Sonoma Valley Bank's regulators, the FDIC and the California Department of Financial Institutions, about the true nature and extent of the bank's lending to the developer and the persons and entities he controlled.

The failure of Sonoma Valley Bank caused in excess of $20 million in losses to taxpayers, approximately $11.47 million to the FDIC, and $8.65 million to the Troubled Asset Relief Program.

Banamex USA Enters into a Non-Prosecution Agreement and Agrees to Forfeit $97.44 Million

On May 22, 2017, Banamex USA (BUSA) agreed to forfeit $97.44 million and entered into a Non-Prosecution Agreement to resolve an investigation into BSA violations.

In its agreement with the Department of Justice, BUSA admitted to criminal violations by willfully failing to maintain an effective anti-money laundering compliance program and willfully failing to file SARs. From at least 2007 until at least 2012, BUSA processed more than 30 million remittance transactions to Mexico with a total value of more than $8.8 billion. During the same period, BUSA's monitoring system issued more than 18,000 alerts involving more than $142 million in potentially suspicious remittance transactions. BUSA, however, conducted fewer than 10 investigations and filed only 9 SARs in connection with these 18,000-plus alerts, filing no SARs on remittance transactions between 2010 and 2012.

BUSA also admitted that, for several years, it should have improved its monitoring of money service business remittances but failed to do so. BUSA employed a limited and manual transaction monitoring system, running only two scenarios to identify suspicious activity on the millions of remittance transactions it processed. These two scenarios produced paper reports that were intended to be reviewed by hand by the two employees assigned to perform the BSA functions of the bank, in addition to time-consuming non-BSA responsibilities. As BUSA began to expand its remittance processing business in 2006, it failed to make necessary improvements to its transaction monitoring controls or add staffing resources.

Former GulfSouth Private Bank President and Two Others Sentenced for Their Roles in Straw Borrower Scheme

On March 10, 2017, the former President of GulfSouth Private Bank in Destin, Florida was found guilty at trial on one count of conspiracy to commit bank fraud, five counts of bank fraud, and one count of mail fraud and later sentenced to 63 months of incarceration followed by 5 years of supervised release for his role in a scheme to hide non-performing loans in the names of straw borrowers. The former senior vice president of GulfSouth Private Bank and a developer also pled guilty on conspiracy and bank fraud charges for their roles in the scheme, and were sentenced to 3 months and 1 day in prison, respectively.

From 2007 to 2012, the two former bank officers conspired with other people, including the developer, to hide non-performing loans in the names of straw borrowers. This assisted in making the bank look more financially stable and kept the loans alive long enough so funds from the Troubled Asset Relief Program could be used to write off some of the losses. Specifically, the former bank officers solicited four bank customers, including the developer, to obtain loans from GulfSouth totaling over $3.8 million and purchase luxury condominium units. In support of the scheme, the former bank officers created and approved false loan documents. The two former bank officers also misled another financial institution into releasing its interest in two of the condominiums.

The other three straw borrowers previously pled guilty and are serving their prison sentences. The former bank president and senior vice president were each ordered to pay $2,421,414 in restitution, jointly and severally with the other subjects in the case. The developer was ordered to pay $627,850 in restitution, jointly and severally with the former bank president and senior vice president.

TOP CHALLENGES FACING THE FDIC AND FOCUS FOR FUTURE OIG WORK

As required by statute, we identified the Top Management and Performance Challenges facing the FDIC. We conducted our research based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from government agencies and officials, and information from private sector entities, in light of the current operating environment and circumstances. Currently, the FDIC is at a critical juncture, particularly with respect to anticipated changes in its leadership and Board of Directors, including the positions of Chair and Vice Chair.

This year, we identified seven areas representing the most significant Challenges for the FDIC. We note that these Challenges will require the constant attention and vigilance by the FDIC for the foreseeable future. In addition, the OIG will focus our limited resources on the highest-risk areas at the FDIC.

Emerging Cybersecurity Risks at Insured Financial Institutions: Cybersecurity is a significant concern for the banking industry because of the industry's use of and reliance on technology, not only in bank operations, but also as an interface with customers. It has become one of the most critical challenges facing the financial services sector due to the frequency and increasing sophistication of cyber attacks. The FDIC has a significant financial interest in mitigating cybersecurity risks at insured banks. If a bank fails, the FDIC will need to step in and may have to fund the losses from the DIF.

Given the significance of cybersecurity risk to U.S. financial institutions, FDIC IT examinations are an important tool to identify weaknesses and vulnerabilities in FDIC-supervised institutions. FDIC IT examinations assess the management of IT risks, including cybersecurity, at FDIC-supervised institutions and at select third-party technology service providers. In September 2016, the FDIC implemented a new Information Technology Risk Examination (InTREx) program for financial institutions. We will be conducting an audit that will assess the InTREx program.

A key challenge associated with IT examinations is ensuring that the FDIC has the right number of examiners with appropriate skills, training, and experience to match institution IT complexity. We are planning to conduct an evaluation of the FDIC's approach to examiner staffing, including IT examination resources.

Management of Information Security and Privacy Programs: Safeguarding computer systems from cyber threats is a high risk across the Federal government and has been a long-standing concern. Without proper safeguards, computer systems are vulnerable to individuals and groups with malicious intentions who can intrude and use their access to obtain sensitive information, commit fraud and identity theft, disrupt operations, or launch attacks against other computer systems and networks.

The FDIC uses IT systems and applications to perform its goals regarding safety and soundness for financial institutions, consumer protection, managing the DIF, and resolution and receivership of failed institutions. These systems and applications hold significant amounts of sensitive data. For example, the FDIC's Failed Bank Data System contains more than 2,500 terabytes of sensitive information from more than 500 bank failures. In addition, FDIC systems contain substantial amounts of PII, including, for example, names, Social Security Numbers, and addresses related to bank officials, depositors, and borrowers at FDIC-insured institutions and failed banks, and FDIC employees. Of the FDIC's 261 system applications, 151 applications required Privacy Impact Assessments because they collect, maintain, or disseminate PII.

Over time, the FDIC has experienced a number of cybersecurity incidents. In August 2011, the FDIC began to experience a sophisticated, targeted attack on its network known as an Advanced Persistent

Threat (APT).[1] The attacker behind the APT penetrated more than 90 workstations or servers within the FDIC's network over a significant period of time, including computers used by the former Chairman and other senior FDIC officials. In late 2015 and early 2016, the FDIC was again impacted by significant cybersecurity incidents. In this case, the FDIC detected seven data breaches as departing employees improperly took sensitive information shortly before leaving the FDIC. The FDIC initially estimated that this sensitive information included the PII of approximately 200,000 individual bank customers associated with approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions; however, the FDIC later revised the number of affected individuals to 121,633.

We will continue to perform the annual review of the FDIC's information security program and practices pursuant to FISMA. We also have work planned in specific areas of the FDIC's information security program.

Utilizing Threat Information to Mitigate Risk in the Banking Sector: The banking sector is vital to public confidence and the nation's safety, prosperity, and well-being. According to Presidential Policy Directive 21, the national preparedness systems must be integrated to secure critical infrastructure, withstand all hazards, and rapidly recover from disasters. Both the Departments of the Treasury and Homeland Security recognized that sharing timely and actionable information is critical to managing risk. In its Annual Report for 2017, the Financial Stability Oversight Council (FSOC) recognized that there was a body of relevant information held by the government that was classified as national security information and must maintain its classification restrictions. Nevertheless, the FSOC encouraged agencies to "balance the need to keep information secure with efforts to share information with industry to enhance cybersecurity resilience."

The financial sector also faces threats based on new technology, such as the rapid growth of the virtual currency markets. At present, the United States does not have a direct and comprehensive program to conduct oversight of the virtual currency markets. Among the challenges identified are the potential for illicit use and connection to criminal activity, legal and supervisory challenges, and integration with and risk to financial institutions. Further, physical threats, such as natural disasters, terrorist attacks, and floods have significant potential to disrupt the financial system. Threats to financial institutions also may come from, or be exacerbated by, their dependence on other critical infrastructure services, such as energy, electricity, communication, and transportation.

Threat information held by the U.S. Government is critical to financial institutions and their service providers. As discussed in FDIC's Supervisory Insights, *A Framework for Cybersecurity*, "financial institutions should have a program for gathering, analyzing, understanding, and sharing information about vulnerabilities to arrive at 'actionable intelligence.'" In order to secure their systems, institutions must have timely and actionable threat information. The financial crisis provided an example of how the default of poorly underwritten mortgages at one bank rippled through the financial system to other

[1] An advanced persistent threat may occur when an entity gains unauthorized access to a computer network, escalates its privileges, and develops an ongoing presence within the network to compromise the network data and component-level security.

banks, brokerages, and insurance companies through asset-backed securities and collateralized debt obligations backed by those mortgages.

Threat information held by the U.S. Government is also critical to FDIC examiners. Examiners should have access to relevant threat information and an understanding of the current threat level and types of threats, in order to focus examinations and prioritize areas for supervisory attention. We intend to perform work that assesses whether examiner personnel and financial institutions have access to threat information that enables them to mitigate risks in their respective roles.

Readiness for Banking Crises: As the financial crisis that began in 2008 unfolded, it challenged every aspect of the FDIC's operations, not only because of its severity, but also because of the speed with which problems unfolded. New vulnerabilities have emerged since the previous financial crisis, and they represent key threats to the financial system. There have been several changes in the financial markets since the crisis – for example: the increased use of automated trading systems, increased speed of executing financial transactions, and a wider variety of trading venues and liquidity providers.

The FDIC must ensure that it has adequate plans in place to address disruptions to the banking system, irrespective of their cause, nature, magnitude, or scope. Further, its plans should be current and up-to-date, and incorporate lessons learned from past crises and the related bank failures. In addition, the plans should contemplate the present and foreseeable state of the banking and financial services sector, as banking industry practices and technologies continue to evolve. Proper authorities, tools, and mechanisms are also needed to address failing institutions in the next crisis.

When resolving a failing or failed bank, the FDIC uses an automated tool called the Claims Administration System (CAS) to identify a depositor's insured and uninsured funds. When planning for the development of the CAS program, the FDIC expected that CAS could make insurance determinations for an institution of any size, up to 5 million deposit accounts; however, over time, the FDIC recognized the challenges of inconsistent and incomplete data at institutions. We have ongoing work to assess to what extent CAS has achieved expectations for accuracy, timeliness, and capacity in making insurance determinations.

Determining the right number and skillsets of permanent staff needed to carry out and support the FDIC's program areas is a fundamental challenge. The FDIC has developed staffing models and operational readiness frameworks to be prepared for both current workload and to deploy resources rapidly in the case of a crisis. A proper infrastructure is also critical in order to address the administrative functions of the agency—such as hiring, contracting, and legal support—in a timely manner. We have work planned to address the FDIC's readiness to respond to any type of crisis.

Enterprise Risk Management (ERM) Practices: ERM is a decision-making tool that assists federal leaders in anticipating and managing risks at an agency, and helps to consider and compare multiple risks and how they present challenges and opportunities when viewed across the organization. According to OMB guidance, ERM is beneficial because it addresses a fundamental organizational issue: the need for information about major risks to flow both vertically (i.e., up and down the organization) and horizontally (i.e., across its organizational units) to improve the quality of decision-making. When

implemented effectively, ERM seeks to open channels of communication, so that managers have access to the information they need to make sound decisions. ERM can also help executives recognize how risks interact (i.e., how one risk can exacerbate or offset another risk). Further, ERM examines the interaction of risk treatments (actions taken to address a risk), such as acceptance or avoidance. We intend to conduct an evaluation of the effectiveness of the FDIC ERM Program.

Acquisition Management and Oversight: Agencies must properly oversee contractor performance and identify any deficiencies, as well ensure appropriate verification of expenditures. Over the last 10 years (2008 through 2017), the FDIC awarded more than 12,600 contracts totaling nearly $11.2 billion.

Contracting Officers are responsible for ensuring the performance of all actions necessary for efficient and effective contracting, compliance with contract terms, and protection of the FDIC's interests in all of its contractual relationships. In addition, FDIC program offices develop contract requirements, and program office Oversight Managers and Technical Monitors oversee the contractor's performance and technical work. Oversight management involves monitoring contract expenses and ensuring that the contractor delivers the required goods or performs the work according to the delivery schedule in the contract.

In our OIG work, we have noted several shortcomings in contractor oversight, which can lead to delays and cost overruns. In our report, *The FDIC's Failed Bank Data Services Project* (March 2017), we reviewed a 10-year, $295 million project related to the transition of the management of failed financial institution data from one contractor to another. Our review focused on transition costs of approximately $24.4 million. The audit concluded that transition milestones were not met, resulting in a one year delay. Further, transition costs, while less than projected in the approval, were greater than the initial estimates at contract inception, by $14.5 million. We concluded that the reasons for the increase were that the FDIC faced challenges related to defining contract requirements, coordinating contracting and program office personnel, and establishing implementation milestones.

We are initiating an evaluation to review FDIC's current contract oversight program.

Measuring Costs and Benefits of FDIC Regulations: In June 2017, the Department of the Treasury issued a report, *A Financial System That Creates Economic Opportunities*, examining costs relating to compliance with regulations imposed on banks. This report recommended that financial regulatory agencies should conduct rigorous cost-benefit analysis and make greater use of proposed rulemaking to solicit public comment. The FDIC generally conducts this analysis on its own initiative for proposed rules.

The Congressional Research Service (CRS) recognized that the use of cost-benefit analysis may improve the quality and effectiveness of federal rules and minimize burden in its *Cost-Benefit and Other Analysis Requirements in the Rulemaking Process* (2014). However, the report notes that performing Cost Benefit Analysis can be a difficult and time-consuming process, and it produces uncertain results because it involves making assumptions about future outcomes. The CRS also noted that cost benefit analysis, "for financial regulation is particularly challenging, due largely to the high degree of uncertainty over precise regulatory costs and outcomes." The report identified three challenges to making accurate

cost benefit analysis: (1) behavioral changes of people as they adapt to a new regulation, (2) quantification that must overcome uncertainty over the causal relationship between the regulation and outcomes, and (3) monetization, which is difficult for outcomes that do not have easily discernable monetary values.

The FDIC faces challenges with proper data collection and lack of available information with respect to measuring costs and identifying benefits for a particular rule and we will continue to monitor the FDIC's efforts in this area.

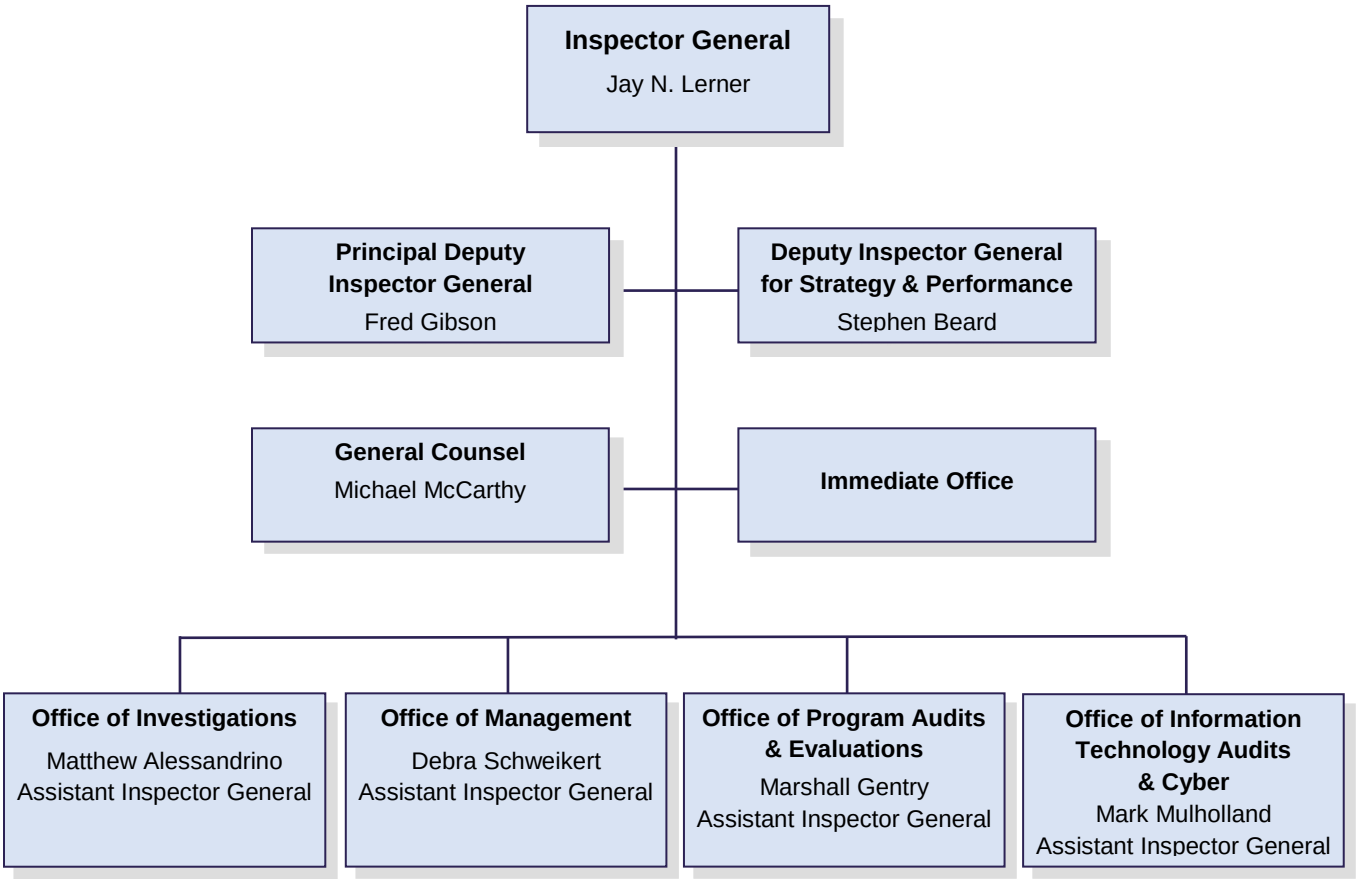
CONCLUSION

The FDIC OIG appreciates the support it has received from the Congress over the past years. We fulfill a critical oversight role at the FDIC and resolve to carry out the OIG mission to preserve the integrity of the agency and banking system. With requested financial resources in FY 2019, we will continue to conduct quality audits and evaluations in accordance with the highest professional standards, issue reports based on reliable evidence and sound analysis, make meaningful recommendations focusing on outcome-oriented impact and cost savings, and follow up to ensure proper implementation of those recommendations. Similarly, in conducting investigations, we will adhere to high professional standards, pursue important and relevant cases with the greatest impact, and maintain positive working relationships with the FDIC and law enforcement partners. Our work in FY 2019 will build on past efforts and focus on the management and performance challenges confronting the FDIC in an ever-changing economic and banking environment. We remain committed to serving the American people as a recognized leader in the Inspector General community.

FDIC OIG Organization Structure and Office Descriptions

The FDIC OIG is comprised of the Inspector General's Immediate Office and component offices as shown below. A brief description of the duties and responsibilities of each component office of the OIG follows:

OIG Organizational Structure and Senior Leadership Team



Field offices are located in Atlanta; Chicago; Dallas; Kansas City; New York; and San Francisco

The **Immediate Office** consists of members of the Inspector General's staff who assist in coordinating with the FDIC Chairman and Board of Directors, strategic planning, communications, Congressional relations, public affairs, and other priority areas.

The **Office of General Counsel** is responsible for providing independent legal services to the Inspector General and the managers and staff of the OIG. Its primary function is to provide legal advice and counseling and interpret the authorities of, and laws related to, the OIG. The General Counsel also provides legal research and opinions; reviews audit, evaluation, and investigative reports for legal considerations; represents the OIG in personnel-related cases; coordinates the OIG's responses to requests and appeals made pursuant to the Freedom of Information Act; coordinates with the FDIC Legal Division where appropriate; prepares IG subpoenas for issuance; and reviews and provides comments on proposed or existing legislation.

The **Office of Program Audits and Evaluations** conducts program evaluations and performance audits to assess the effectiveness and efficiency of FDIC programs and operations. This group also conducts reviews of failed banks and other systemic issues, and compliance audits.

The **Office of IT Audits and Cyber** conducts audits of IT risks and challenges – both internal to the FDIC's own systems, and external to insured banks and the financial sector. This group also works to develop and leverage the OIG's data analytics capabilities to identify the highest-risk areas at the FDIC.

The **Office of Investigations** carries out a nationwide program to prevent, detect, and investigate criminal, civil, or administrative wrongdoing and misconduct by FDIC employees and contractors. This group operates an Electronic Crimes Unit and forensic laboratory, and assists in responding to OIG Hotline allegations of suspected fraud, waste, abuse, and mismanagement.

The **Office of Management** is the management operations arm of the OIG with responsibility for providing business support for the OIG, including financial resources, human resources, OIG websites, contracting and acquisition, records retention, internal controls, and OIG policies and directives.

OIG Accomplishments in FY 2017

In FY 2017, results of OIG audits, evaluations, and investigations were as follows:

Significant Outcomes (October 1, 2016 –September 30, 2017)	
Audit and Evaluation Reports Issued	13
Questioned Costs or Funds Put to Better Use	$126,593
Recommendations	63
Investigations Opened	84
Investigations Closed	106
Judicial Actions:	
Indictments/Informations	122
Convictions	101
Arrests	40
OIG Investigative Results:	
Fines	$442,000
Restitution Ordered	98,026,963
Asset Forfeitures	121,272,872
Civil Recoveries	11,525,428
Total	**$231,267,263**

Budget Request for FY 2019

Appropriation Bill Language
For necessary expenses of the Office of Inspector General in carrying out the provisions of the Inspector General Act of 1978, as amended, $42,982,000 to be derived from the Deposit Insurance Fund.

Object Classification	FY 2017 Actual (000 omitted)	FY 2018 Budget (000 omitted)	FY 2019 Proposed (000 omitted)
11.1 Full-Time Equivalent	$20,410	$22,858	$24,049
11.5 Other Personnel Compensation	802	1,000	947
11.9 Total Personnel Compensation	$21,212	$23,858	$24,996
12.0 Civilian Personnel Benefits	9,333	10,473	11,930
21.0 Travel and Transportation of Persons	1,272	1,595	1,307
22.0 Transportation of Things	26	28	14
24.0 Printing and Reproduction	0	0	0
25.0 Other Services *	2,247	2,197	1,827
26.0 Supplies and Materials	15	15	17
31.0 Equipment	1,027	970	2,891
Total Appropriation	**$35,132**	**$39,136**	**$42,982**

Personnel Summary	FY 2017 Actual	FY 2018 Budget	FY 2019 Proposed
Total Compensable Work Years:			
Staffing	128	144	144

* Other Services in FY 2019 includes $250,000 for training and $94,000 for support of the Council of the Inspectors General on Integrity and Efficiency.