governmentattic.org
"Rummaging in the government's attic"

Description of document:	Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) fiscal year (FY) 2018 proposed budget, May 2017
Requested date:	20-August-2017
Released date:	02-October-2017
Posted date:	13-November-2017
Source of document:	FOIA Request Federal Deposit Insurance Corporation FOIA/Privacy Act Group, Legal Division 550 17th Street, NW Washington, DC 20429-9990 Submit Electronic FOIA Request

The governmentattic.org web site ("the site") is noncommercial and free to the public. The site and materials made available on the site, such as this file, are for reference only. The governmentattic.org web site and its principals have made every effort to make this information as complete and as accurate as possible, however, there may be mistakes and omissions, both typographical and in content. The governmentattic.org web site and its principals shall have neither liability nor responsibility to any person or entity with respect to any loss or damage caused, or alleged to have been caused, directly or indirectly, by the information provided on the governmentattic.org web site or in this file. The public records published on the site were obtained from government agencies using proper legal channels. Each document is identified as to the source. Any concerns about the contents of the site should be directed to the agency originating the document in question. GovernmentAttic.org is not responsible for the contents of documents published on the website.

-- Web site design Copyright 2007 governmentattic.org --

Federal Deposit Insurance Corporation
550 17th Street, NW, Washington, DC 20429-9990
Legal Division

October 2, 2017

RE: FDIC FOIA Request Log Nos. 17-0395

This is our final response to your August 20, 2017 Freedom of Information Act (FOIA) request, received by the FDIC's FOIA/Privacy Act Group on August 31, 2017, for "a copy of the congressional budget justification for the FDIC Office of Inspector General."

We reasonably interpreted your request to be for the Fiscal Year 2018 Budget of the FDIC Office of Inspector General ("OIG 2018 Budget").

Your request has been granted.

Our records search has been completed, and the OIG 2018 Budget has been located.

The OIG 2018 Budget is being disclosed to you in its entirety. A copy of the OIG 2018 Budget (23 pages) is enclosed.

This completes the processing of your request, which has been processed at no cost to you.

You may contact me at jsussman@fdic.gov or 703-562-2039 or our FOIA Public Liaison, FDIC Ombudsman M. Anthony Lowe at MLowe@FDIC.gov or by telephone at (312) 382-7552, for any further assistance and to discuss any aspect of your request.

Sincerely,

/signed/

Jerry Sussman, Senior FOIA Specialist
FOIA/Privacy Act Group

Enclosure:
OIG 2018 Budget (23 pages).

Office of Inspector General

Fiscal Year 2018 Budget

May 2017

Table of Contents

Office of Inspector General
Fiscal Year 2018 Budget

This document presents the Federal Deposit Insurance Corporation (FDIC) Office of Inspector General's (OIG) fiscal year (FY) 2018 proposed budget. To provide perspective and context for our budget needs and planned areas of focus for FY 2018, we also include information on our FY 2017 activities and our overall accomplishments during FY 2016.

Unprecedented events and turmoil in the economy and financial services industry during the financial crisis affected every facet of the FDIC and its operations, posing challenges both to the Corporation and our office. Changes in economic conditions more recently have stabilized the financial services sector. We have examined the post-crisis environment at the FDIC and are focusing our efforts on current and emerging risks to the FDIC and the banking industry. We appreciate the past support of our stakeholders and look forward to continuing our audits, evaluations, and investigations, and working closely with the FDIC, the Congress, other OIGs, and federal law enforcement colleagues to help ensure the successful accomplishment of the OIG's and FDIC's mission.

MISSION AND VISION

The Congress created the FDIC in 1933 to restore public confidence in the nation's banking system. The FDIC insures deposits at 5,913 banks and savings associations and it promotes the safety and soundness of these institutions by identifying, monitoring, and addressing risks to which they are exposed. The FDIC receives no federal tax dollars – insured financial institutions fund its operations. Passage of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) made permanent the $250,000 standard maximum deposit insurance limit that had been increased temporarily from $100,000 during the financial crisis.

The FDIC OIG is an independent and objective unit established under the Inspector General (IG) Act of 1978, as amended. Jay N. Lerner was sworn in as the FDIC IG on January 9, 2017. The OIG's mission is to promote the economy, efficiency, and effectiveness of FDIC programs and operations, and protect against fraud, waste, and abuse to assist and augment the FDIC's contribution to stability and public confidence in the nation's financial system. In carrying out its mission, the OIG

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

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. CIGFO may also convene working groups to evaluate the effectiveness of internal operations of FSOC. Additionally, we meet with representatives of the Government Accountability Office to coordinate work and minimize duplication of effort. 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 and pursue matters of mutual interest.

Appendix I presents an overview of the OIG's current organizational structure and a more detailed description of our component offices. Importantly, in early April 2017, the IG announced a reorganization of the FDIC's former Office of Audits and Evaluations. Having considered the challenges facing the FDIC, particularly in the information security and cyber realms, the IG established two new offices and reassigned former audit and evaluation staff. Specifically, the **Office of IT Audits and Cyber** now 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. The **Office of Program Audits and Evaluations** conducts program evaluations and performance audits to assess how effectively FDIC is achieving its goals and objectives. This group also conducts reviews of failed banks and other systemic issues, and compliance audits.

With respect to statutorily required FDIC OIG work, an important responsibility for our office is to perform various reviews of failed FDIC-supervised depository institutions under the provisions of the Federal Deposit Insurance Act, as amended by the Dodd-Frank Act. Annually, the OIG reviews the FDIC's information security program and practices pursuant to the Federal Information Security Modernization Act of 2014 (FISMA). In addition, to satisfy Digital Accountability and Transparency Act of 2014 (DATA Act) IG reporting responsibilities, we will be reviewing statistical samples of data submitted by the FDIC under the Act and reporting on the completeness, timeliness, quality, and accuracy of the data.

We conduct other audits and evaluations of areas where we identify risks to FDIC programs and operations. We also pursue investigations of criminal activity affecting FDIC-insured institutions and other investigative activities to ensure integrity in the banking system and the FDIC.

The OIG's vision is to be a quality-focused FDIC team that promotes excellence and trust in service to the Corporation and the public interest. The OIG strives to address issues of significance to the Corporation, the Congress, the financial services industry, and the American people. Appendix II presents a brief summary of FY 2016 accomplishments on which we continue to build in our ongoing and planned work.

OIG FUNDING

The FDIC OIG is the only appropriated unit in the FDIC. The OIG has been operating under an appropriated budget since FY 1998 in accordance with Section 1105(a) of Title 31, United States Code, which provides for "a separate appropriation account for appropriations for each Office of Inspector General of an establishment defined under Section 11(2) of the Inspector General Act of 1978."

The OIG's budget is authorized through the Congressional appropriations process with the funds derived from the Deposit Insurance Fund (DIF). It is also reflected in the FDIC's corporate budget and approved by the FDIC Chairman as part of the Corporation's budget formulation process.[1] 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.

PROPOSED FISCAL YEAR 2018 BUDGET

The OIG's proposed FY 2018 budget includes funding totaling $39.136 million. The budget supports an authorized staffing level of 144.

The majority of requested funds support personnel costs and benefits:

- $23.858 million, or 61 percent, for salaries and
- $10.473 million, or 26.8 percent, for personnel benefits.

The remaining $4.805 million, or 12.3 percent, is for non-personnel costs, of which $1.595 million, or 4.1 percent, is designated for travel costs, and $1.75 million, or 4.5 percent, for a portion of other services, including contractors that we engage to assist in accomplishing our mission. Also included in other services are expenses such as $250,000 for training, $78,000 to support statutorily required contributions to the Council of the Inspectors General on Integrity and Efficiency, and miscellaneous expenses of $119,000. Additionally, we are requesting $970,000, or 2.5 percent, for IT equipment and $43,000 for other operating costs. Appendix III presents our FY 2018 Appropriation Bill Language, Object Classification, and Personnel Summary.[2]

In planning for FY 2018 and the future, we are revising all of our component office longer-range strategic plans to ensure they align with the DIG's mission under the Inspector General Act, that our work addresses the most significant risk areas, and that our human and financial resources are sufficient to address those risks. This process includes identifying projects and products that will add the most value to the FDIC; assessing our IT and related security needs; examining our investigative caseload and related activities to be sure they are yielding the best possible outcomes; and revisiting our internal business processes, policies, and procedures to ensure they provide effective and efficient guidance for all aspects of our work. To date, our planning for FY 2018 has identified a number of important IT-related initiatives and priorities where funding would likely be directed, for example: enhancements to our Electronic Crimes Unit, planning for development of a robust data analytics capability, external website improvements, E-Discovery activities, and strengthened security features for our internal IT operations.

---

1 The corporate budget does not provide the OIG with any additional funding but instead provides the Corporation with an estimate of OIG expenses in accordance with the appropriated budget as approved by the Congress.

2 The FDIC OIG receives a lump-sum appropriation for "necessary expenses of the Office of Inspector General in carrying out the provisions of the Inspector General Act of 1978." Appendix III represents the FDIC OIG's best estimate of our needs during the appropriations period, but the OIG may modify specific allocations, as needed.

Our planning will be ongoing and, in order to be successful, will continue throughout the current fiscal year and into FY 2018. We would note also that our strategic planning initiative is in line with the principles outlined in the current Administration's OMB M-17-22, *Comprehensive Plan for Reforming the Federal Government and Reducing the Federal Civilian Workforce*.

AUDIT AND EVALUATION PRIORITIES

The following discussion focuses on the FDIC's operating environment and the FDIC OIG's recently completed, ongoing, or planned audit and evaluation work in key areas.

Information Technalagy Security and Gavernance

Essential to achieving the FDIC's mission of maintaining stability and public confidence in the nation's financial system is safeguarding sensitive information, including personally identifiable information (PII) that the FDIC collects and manages in its role as employer, federal deposit insurer, regulator of state nonmember financial institutions, and receiver of failed institutions. Materials that the FDIC possesses related to its Dodd-Frank Act responsibilities contain some of the most sensitive information that the FDIC maintains, and safeguarding it from unauthorized access or disclosure is critically important. Equally important to the FDIC and the Nation is the defense of critical infrastructure, which includes financial systems and associated computer network operations. In that regard, the Federal Information Security Modernization Act (FISMA) of 2014 establishes standards to assess information security government wide. The OIG's FISMA work is intended not only to ensure compliance with those standards but also to help defend the critical infrastructure against those who would attack it.

In recent years, the FDIC OIG has increased its focus on the FDIC's IT security and governance, and we consider this area a top priority. In fact, going back to August 2011, the FDIC began investigating a sophisticated, targeted attack on its network known as an Advanced Persistent Threat (APT). The incidents associated with the APT were among the most significant that the FDIC investigated between 2011 and 2013. In our November 2013 FISMA audit report, we concluded that the FDIC did not comply with federal or FDIC policies and procedures when responding to the APT. We also found that the FDIC's incident response program policies and procedures did not adequately address complex, targeted incidents and lacked a risk framework for escalating incidents to senior management. Further, the FDIC's response to the APT focused primarily on implementing technological solutions and did not include an adequate assessment of the associated risk from a corporate perspective. In response to a recommendation in our FISMA report, the FDIC revised its incident response policies and procedures to address complex incidents, such as APTs, and clarified the role of the FDIC's security staff in investigating and responding to such incidents.

In July 2016, our office completed two audits related to the unauthorized exfiltration of sensitive information, including PII. The first audit focused on the FDIC's controls for identifying and reporting major information security incidents. As part of that audit, we reviewed the FDIC's investigative activities, records, decisions, and reports for a data breach that we termed "the Florida Incident." We found that although the FDIC had established various incident response policies, procedures, guidelines, and processes, these controls did not provide reasonable assurance that major incidents would be

identified and reported to the Congress in a timely manner, as required by FISMA. We made recommendations that the FDIC is working to address, involving: revising and updating incident response policies, procedures, and guidelines, reviewing the implementation of the Data Loss Prevention tool to determine how the tool can be better leveraged to safeguard sensitive information and identify and mitigate major incidents, and establishing a process to ensure that future Congressional notifications of major incidents include appropriate context.

The results of our audit prompted the CIO to initiate a review of similarly-situated security incidents to determine whether additional incidents warranted designation as major. The review resulted in six additional incidents being reported to the Congress as major between March and May 2016. We are currently performing a special inquiry review in response to a request from the Committee on Banking, Housing, and Urban Affairs, U.S. Senate, to further examine the circumstances surrounding the FDIC's identifying and reporting on all of the incidents, along with other related assignments that are listed below as ongoing.

In a second audit, we reviewed FDIC's safeguarding of resolution plans submitted under the Dodd-Frank Act. This work 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. The FDIC subsequently formally established an insider threat and counterintelligence program.

The Acting Inspector General (IG) at the time testified regarding these matters on two occasions—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.

FISMA 2016: Finally, with respect to completed work in this area, our 2016 FISMA work determined that the FDIC had established a number of information security program controls and practices that were generally consistent with FISMA requirements, Office of Management and Budget (OMB) policy and guidelines, and applicable National Institute of Standards and Technology standards and guidelines. The FDIC had also taken steps to strengthen its security program controls following our 2015 FISMA work.

Notwithstanding these actions, our FISMA audit found security control weaknesses that impaired 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 elevated risk. Some findings were identified during the current year and others were identified in prior reports issued by the OIG or the Government Accountability Office. We identified areas of notable weakness that required attention, among those: strategic planning, vulnerability scanning, the FDIC's information security manager program, configuration management, third-party software patching, multifactor authentication, and contingency planning.

We also pointed out risks related to the performance of the vendor that supports the FDIC's infrastructure services, commented on the frequent turnover in the Chief Information Security Officer (CISO) position, and questioned whether the CISO's authorities enable the CISO to effectively address the responsibilities defined in FISMA. During our 2017 FISMA assignment, which is ongoing, we will examine progress made in these areas. We will also assess the FDIC's incident response controls as part of this audit.

Other ongoing IT-related assignments for FY 2017 and into FY 2018, include the following:

- **Governance of Information Technology Initiatives**. The audit is focusing on the FDIC's IT governance structure, enterprise architecture, and strategic plans in relation to selected IT initiatives, including the planned migration of email to the cloud, the deployment of laptop computers to FDIC employees and contractor personnel, and the potential adoption of a managed services solution for mobile IT devices.
- **Controls for Preventing and Detecting Advanced Persistent Threats (APT):** An APT is a network attack in which an unauthorized entity gains access to the network and stays there undetected for a long period of time, with the intent of stealing data. APTs can pose serious threats to the FDIC's mission and to the financial services industry as a whole. Our work in this area will examine the controls currently in place at the FDIC to prevent and detect such attacks.
- **FDIC Controls over Separating Employees' Access to Sensitive Information:** This review will determine the extent to which the FDIC has implemented controls to mitigate the risk of unauthorized access to and inappropriate removal and disclosure of sensitive information by separating employees and contractors.
- **The FDIC's Controls for Responding to a Suspected or Confirmed Breach of Personally Identifiable Information (PII):** This audit is assessing the adequacy of the FDIC's processes for evaluating the risk of harm to individuals potentially affected by a breach involving PII and its processes for notifying and providing services to those individuals, when appropriate.
- **Security Configuration Changes and Software Updates to the FDIC's Windows Servers:** This work will determine whether the FDIC has established and implemented change management controls over its Windows Server operating system software that are consistent with federal requirements and guidelines.

We are currently developing an **IT Strategic Plan** to guide our efforts in this area going forward.

Systemic Resolution Responsibilities

The Dodd-Frank Act created a comprehensive new regulatory and resolution framework designed to avoid the severe consequences of financial instability. Under current law, Title I of the Dodd-Frank Act provides tools for regulators to impose enhanced supervision and prudential standards on systemically important financial institutions (SIFI). Title II provides the FDIC with a new orderly liquidation authority for SIFIs, subject to a systemic risk determination by statutorily designated regulators.

SIFI Proximity and Speed to Default: We recently evaluated the progress the FDIC has made in developing criteria and a process for assessing SIFIs' proximity and speed to default or danger of default

so that it is positioned to undertake necessary preparatory actions for a SIFI resolution. We determined that the FDIC had made steady progress in developing criteria and a process, namely the Systemic Monitoring System (SMS), for assessing the proximity and speed to default for the 16 large and complex SIFIs with assets over $13 trillion that were in the FDIC's portfolio as of June 2016. The SMS gathers and analyzes SIFI supervisory reports and market information using standardized metrics that are then combined with FDIC onsite institution monitoring teams' perspectives and analyses of the risks shown by those metrics. Ultimately, an FDIC committee assesses the indicated risks from institution monitoring team submissions and other sources to assign a quarterly risk rating for each SIFI on its proximity and speed to default. As the proximity to default increases, the FDIC may take a number of actions, including increased monitoring and a resolution strategy refresh.

We made three recommendations relating to improving SMS documentation and independently evaluating the SMS tool's output. Management agreed to take corrective action.

CIGFO Joint Audit: We also joined fellow members of the Council of Inspectors General on Financial Oversight in conducting a joint audit of the *Financial Stability Oversight Council's Efforts to Promote Market Discipline.* The report concluded that FSOC has made progress in promoting market discipline. However, the wide range of views that still exist on the issue of "too big to fail" indicate that there is a lack of consensus regarding whether FSOC has eliminated expectations on the part of shareholders, creditors, and counterparties of large bank holding companies or nonbank financial companies that the federal government will shield them from losses in the event of failure.

Added OIG Responsibilities Under the Dodd-Frank Act: We would also note that under current law, the Dodd-Frank Act requires that the FDIC IG conduct, supervise, and coordinate audits and investigations of the liquidation of any covered financial company by the Corporation as receiver under Title II of the Act. These reviews must occur not later than 6 months after the date of appointment of the Corporation as receiver under this title and every 6 months thereafter. We are monitoring possible changes to Title II requirements and will respond accordingly.

The FDIC's Supervisory Responsibilities

The FDIC's supervision program promotes the safety and soundness of FDIC-supervised insured depository institutions. The FDIC is the primary federal regulator for 3,787 FDIC-insured, state-chartered institutions that are not members of the Board of Governors of the Federal Reserve System. As such, the FDIC is the lead federal regulator for the majority of community banks.

In light of technological changes, increased use of technology service providers (TSP), new delivery channels, and cyber threats, we have pointed out in past work that the FDIC's IT examination program needs to be proactive and bankers and Boards of Directors need to ensure a strong control environment and sound risk management and governance practices in their institutions. Importantly, with respect to TSPs, one TSP can service hundreds or even thousands of financial institutions, so the impact of security incidents in one TSP can have devastating ripple effects on those institutions. Controls need to be designed not only to protect sensitive customer information at banks and TSPs, but also to guard against

intrusions that can compromise the integrity and availability of operations, information and transaction processing systems, data, and business continuity.

TSP Contracts with FDIC-Supervised Institutions: In February 2017 we issued an evaluation report regarding certain aspects of TSP contracts with FDIC-supervised institutions. Many banks use TSPs to support critical business needs, such as core processing, loan servicing, accounting support, or data management. The report assessed how clearly FDIC-supervised institutions' contracts for these services addressed the TSP's responsibilities related to business continuity planning, and responding to and reporting on cybersecurity incidents.

We reviewed a sample of 48 TSP contracts from 19 financial institutions (FI). We did not see documentary evidence that most of the FDIC-supervised financial institutions fully considered and assessed the potential impact and risk that TSPs may have on the institution's own business continuity planning, and incident response and reporting. In this regard, documentation supported that only 8 of the 19 institutions completed both a risk assessment and contract review to understand the business and legal risks, as recommended by supervisory guidance. Further, when completed, the quality of these assessments varied.

Most of the contracts we reviewed did not clearly address the TSP's responsibilities and lacked specific provisions to protect certain key FI interests or preserve FI rights. Nearly half of the contracts did not require the TSP to establish a business continuity plan. Most contracts also did not sufficiently define key terminology related to business continuity and incident response. Therefore, these TSP contracts provided FIs with limited information and assurance that TSPs could recover and resume critical systems, services, and operations timely and effectively, if disrupted; and would take appropriate steps to contain and control incidents and report them in a timely manner.

The FDIC independently – and the Federal Financial Institutions Examination Council (FFIEC) members collectively – have taken numerous steps to provide institutions comprehensive business continuity, cybersecurity, and vendor management guidance, as well as to enhance related examination programs. Notwithstanding these steps, our evaluation results indicate that more time is needed to allow FDIC and FFIEC efforts to have an impact.

We recommended that the FDIC continue communication efforts with FIs regarding the risks posed by TSP contracts; and after allowing for a reasonable period of time for FIs to incorporate FDIC and FFIEC guidance, that the FDIC conduct a follow-on study to assess the extent to which financial institutions have effectively addressed key issues related to risks posed by TSP contracts. FDIC management concurred with our recommendations.

Reviews of Failed Banks: With respect to other OIG work in the supervision area, we continue to conduct material loss reviews (MLR), failed bank reviews (FBR), and in-depth reviews of failed institutions, as appropriate. As noted earlier, under the Dodd-Frank-Act, our office must conduct MLRs of FDIC-supervised institutions whose failures cause a loss to the DIF exceeding $50 million and conduct an FBR of each institution with a DIF loss at or below the MLR threshold to determine if unusual circumstances warrant the OIG conducting an in-depth review of the loss. The goal of our work

involving failed banks is to continue to shed light on the circumstances that caused such failures and ways in which the FDIC's supervisory activities can be enhanced to avoid future failures. We have completed four FBRs during FY 2017 to date and currently have two MLRs in process--that of Seaway Bank and Trust, Chicago, Illinois, which failed on January 27, 2017, with an estimated loss to the DIF of $57.2 million and an MLR of First NBC Bank, New Orleans, Louisiana, which failed on April 28, 2017, with a $996.9 million estimated loss to the DIF.

Other ongoing assignments addressing the FDIC's supervisory responsibilities include the following:

- **The FDIC's Risk Management Examination Loan Sampling Methodology**: We are evaluating the FDIC's loan sample selection methodology, including compliance with examiner guidance, and the extent to which examiner loan samples are representative of financial institutions' loan risk exposures.
- **Forward Looking Supervision for High Growth-High Concentration Institutions:** This work will be designed to determine the extent to which the FDIC's forward-looking supervision initiative has affected the supervisory response to institutions that have experienced high growth and/or that have high commercial real estate or acquisition, development, and construction loan concentration risk.

Resolution ond Receivership Responsibilities

One of the FDIC's most important roles is acting as the receiver or liquidating agent for failed FDIC-insured institutions. The FDIC's responsibilities include planning and handling the resolutions of failing FDIC-insured institutions and providing prompt, responsive, and efficient administration of failing and failed financial institutions in order to maintain confidence and stability in our financial system.

As part of the resolution process, the FDIC values a failing federally insured depository institution, markets it, solicits and accepts bids for the sale of the institution, considers the least costly resolution method, determines which bid to accept, and works with the acquiring institution through the closing process. The receivership process involves performing the closing function at the failed bank; liquidating any remaining assets; and distributing any proceeds to the FDIC, the bank customers, general creditors, and those with approved claims.

The FDIC places great emphasis on promptly marketing and selling the assets of failed institutions and terminating the receivership quickly. Although the number of institution failures has fallen dramatically since the crisis, these activities still pose challenges to the Corporation. As of December 31, 2016, the FDIC's Division of Resolutions and Receiverships (DRR) was managing 378 active receiverships with assets in liquidation totaling about $3.3 billion.

In addition, through purchase and assumption agreements with acquiring institutions, the Corporation has entered into shared-loss agreements (SLA). Since November 2008, the Corporation has resolved 304 failures with accompanying SLAs. Under these agreements, the FDIC agrees to absorb a portion of the loss—generally 80 to 95 percent—which may be experienced by the acquiring institution with regard to those assets, for a period of up to 10 years. The FDIC entered into 304 SLAs from November 2008

through September 30, 2013, with an initial asset base of $216.5 billion. As of December 31, 2016, FDIC recoveries totaled $5.2 billion, representing 15.1 percent of the $34.2 billion in FDIC SLA payments.

Our work in the resolutions and receivership areas during FY 2017 has addressed SLA recoveries and the FDIC's Failed Bank Data System (FBDS), a system that the FDIC uses for receivership purposes.

SLA Recoveries: With respect to SLAs, we initiated an evaluation based on the risks associated with assuming institutions identifying and remitting SLA recoveries to the FDIC. An increasing number of Commercial SLAs are becoming 5 years old, resulting in the end of SLA loss coverage but not the end of the 8-year recovery period, during which assuming institutions (AI) are required to remit a portion of their recoveries to the FDIC. Our evaluation assessed the FDIC's efforts to ensure that AIs identify and remit SLA recoveries to the FDIC. A recovery typically comprises (1) funds paid by the borrower on assets that the AI previously charged off or experienced a loss on and received reimbursement from the FDIC pursuant to an SLA; or (2) gains from the sale of foreclosed property or SLA assets.

We determined that the FDIC's DRR established controls to mitigate risks and help ensure AIs appropriately identify and remit recoveries to the FDIC. These controls include a process for identifying recovery and non-recovery assets and conducting on-site reviews that focus on recoveries. DRR also issued guidance and provided training to DRR employees, assuming institutions, and third-party contractors that DRR engages to complement its staff. The guidance and training communicate recovery period procedures and expectations.

A contractor that we engaged to test a sample of SLA assets pertaining to five AIs that we selected found several discrepancies. The contractor identified an unreported recovery of $16,423 at one AI as a result of an isolated oversight. The AI agreed with the finding and reimbursed the FDIC for the recovery, following the contractor's review. The contractor found several other instances where an AI had overpaid the FDIC.

We made several recommendations to ensure AIs accurately identify and report SLA recoveries to the FDIC and that the FDIC review a sample of SLA certificates to identify any payment errors similar to those identified in this evaluation. The FDIC concurred with our recommendations.

Status of FBDS: More recently, we issued an audit report regarding the status of the FBDS project. The FBDS project established a new contract and system for maintaining records of failed financial institutions that the FDIC obtains as receiver. Maintaining such records is critically important, as various internal and external parties, including outside counsel, use them to support investigations, litigation, tax administration, and asset sales. The report assessed the status of the project, including progress and costs in relation to goals, budgets, and milestones; factors contributing to the project's progress; and outstanding risks that must be addressed.

While the FDIC had a number of significant achievements associated with the FBDS project, we found that the project had not met key milestones and costs exceeded estimates. Specifically, there was a delay in implementing certain system capabilities and transitioning data from the prior contractor's system to the FBDS system. The transition-related schedule delays caused the FDIC to extend the prior

contract several times into 2016—beyond the initially anticipated contract expiration date. As a result of those extensions, and other challenges, the FDIC absorbed about $14.6 million more in transition-related costs than had been estimated. Dverall, total transition-related costs remained less than what was originally projected when the FDIC Board of Directors approved the project.

We identified three factors contributing to the project's status. Specifically, FDIC personnel did not fully understand the project's scope and requirements, did not establish clear expectations for the project in contract documents, and did not implement a project management framework to guide and structure project activities. FDIC personnel identified other factors that impacted the project's delays, including technical challenges and the unanticipated failure of a large, complex financial institution.

Dur office made seven recommendations to strengthen FBDS governance, project management, and contract oversight to reduce FBDS project-related risks going forward. FDIC management concurred with our recommendations.

Finally, we recently initiated a review of the **FDIC's Claims Administration System**. FDIC personnel use the claims system to identify insured and uninsured deposits in failing and failed financial institutions. This system is critical to achieving the FDIC's mission to insure deposits and administer receivership claims.

Consumer Protection

The FDIC carries out its consumer protection role by providing consumers with access to information about their rights and disclosures that are required by federal laws and regulations. Its Consumer Response Center serves an important function in this regard. Importantly, the FDIC also examines the banks for which it is the primary federal regulator to determine the institutions' compliance with laws and regulations governing consumer protection, fair lending, and community investment. These activities require effective examiner training and regular collaboration with other regulatory agencies.

The Dodd-Frank Act consolidated many of the consumer financial protection authorities previously shared by several federal agencies into the Consumer Financial Protection Bureau (CFPB) and granted the CFPB authority to conduct rulemaking, supervision, and enforcement with respect to federal consumer financial laws; handle consumer complaints and inquiries; promote financial education; research consumer behavior; and monitor financial markets for risks to consumers. The FDIC coordinates with the CFPB on consumer issues of mutual interest and to meet statutory requirements for consultation relating to rulemakings in mortgage lending and other types of consumer financial services and products.

We currently have two assignments ongoing in the consumer protection area:

- **The FDIC's Consumer Response Center:** We are assessing the FDIC's handling of consumer complaints, in particular--how the FDIC receives, investigates, analyzes, and responds to consumer complaints involving FDIC-supervised institutions and how it identifies emerging issues and trends, and takes action accordingly.

- **The FDIC's Implementation of Consumer Protection Laws Regarding the Ability to Repay Mortgage Loans and Loan Originator Compensation:** We are assessing the FDIC's efforts in implementing changes to several existing federal consumer financial laws requiring rulemaking and changes to industry practices and compliance examinations. These changes were brought about with passage of the Dodd-Frank Act. We will look specifically at the rules that direct financial institutions to determine if a consumer has a reasonable ability to repay a mortgage loan and rules to place limits on loan originator compensation.

The FDIC's Resources Management and Business Operations

As the number of financial institution failures continues to decline, the FDIC has been reshaping its workforce and adjusting its budget and human resources as it seeks a balanced approach to managing costs while achieving mission responsibilities. The FDIC Board of Directors approved a $2.16 billion Corporate Dperating Budget for 2017, 2.4 percent lower than the 2016 budget. In conjunction with its approval of the 2017 budget, the Board also approved an authorized 2017 staffing level of 6,363 positions for 2017, a 2.6 percent decrease from 2016 and 32 percent lower than the peak in 2011. This was the seventh consecutive reduction in the FDIC's annual operating budget.

As conditions improve throughout the industry and the economy, the FDIC will strive to achieve the appropriate level of resources, and at the same time, it needs to continue to carry out its day-to-day operations in an efficient, effective, and economical manner. In this regard, the OIG has devoted resources to many facets of the business operations and programs of the FDIC during 2017. We have completed several assignments and others are ongoing, as described below.

Employee Travel: We initiated an evaluation in response to two OIG Hotline complaints regarding employee travel. The complainants alleged that certain FDIC employees were (1) traveling excessively and unnecessarily at the FDIC's expense; (2) designated as Work in Place (WiP), but incurring significant commuting expenses; and (3) traveling frequently enough to invoke tax consequences that were not addressed by the FDIC and the employees involved. We reviewed business travel completed by seven FDIC employees identified in the complaints and developed statistics on business travel completed by 125 employees identified as WiP by the FDIC.

We concluded that some of the allegations involving the travel patterns of the seven FDIC employees had merit. Five employees were designated as WiP and traveled frequently to their reporting duty station in Washington in 2015, contrary to the intent of the WiP program. (One of the seven employees was not WiP and did not travel frequently or extensively.) Three of the five WiP employees traveled extensively to Washington under details or promotions exceeding 1 year, which could trigger tax consequences. The Corporation began withholding taxes for one of those employees when it became apparent that the employee's detail and related travel would exceed 1 year. We reported that FDIC management should review the facts and circumstances for the other two WiP employees and determine whether withholding is warranted.

The seventh employee named in the allegation was an FDIC Executive that the FDIC reimbursed for extensive travel to his original city of residence, which was near an FDIC office (an Alternate Location),

over a 14-year period. The Executive had relocated from the Alternate Location to Washington and had operated under an informal work arrangement since 2002 that allowed him to spend a portion of his work time in the Alternate Location, where he continued to maintain a residence. In addition to receiving relocation benefits, the Executive earned a Washington-based salary that was 17-percent higher than what he would have earned in the Alternate Location in 2016.

In our view, the work arrangement created risks and adverse consequences for the Corporation and potentially for the Executive and appeared not to be in the FDIC's best interests. Our report discusses several factors that contributed to this situation, including the Executive's former supervisor's decision to allow the work arrangement and the unique and informal nature of the arrangement. The work arrangement involved unusual provisions and was difficult to monitor, lacked parameters and controls, and created the risk of expenses that outweighed business needs. It would have been prudent for management to periodically review whether the arrangement continued to provide sufficient value to the Corporation.

We also concluded that the Executive took frequent advantage of the work arrangement for his own personal benefit and convenience. We questioned the necessity and reasonableness of $122,423 in costs associated with the Executive's travel to the Alternative Location.

We made eight recommendations to strengthen policy and controls surrounding long-term taxable travel, the WiP program, and processes for identifying and monitoring unusual or questionable travel patterns. We also recommended that the FDIC disallow and attempt to recover $122,423 in costs associated with the Executive's travel to the Alternate Location.

FDIC management concurred with seven recommendations and partially concurred with our recommendation to disallow and attempt to recover costs. The FDIC reviewed the Executive's travel patterns and facts associated with travel to the Alternate Location, recovered $2,658 in charges it concluded were not permitted under the work arrangement, and determined the remaining travel expenses were authorized under the work arrangement.

Contract Audit of Lockheed Martin Services, Inc.: The FDIC's contracting activities are another area where the OIG has focused resources. For example, and as referenced earlier with respect to the Failed Bank Data Services project, to accommodate the enormous data conversion and storage demands associated with the large number of institution failures in recent years, the FDIC entered into a contract with Lockheed Martin Services, Inc. for data management services. Under the contract, Lockheed provided the FDIC with a standard method of maintaining failed institution data, including secure data migration, conversion, cataloging, indexing, storage, security, and retrieval.

Earlier this year we engaged a contractor to audit invoices submitted by Lockheed to determine whether charges paid by the FDIC to Lockheed were adequately supported, allowable under the terms and conditions of the contract and task orders, and allocable to their respective task orders.

The contractor determined that all but $124 of the $17,478,331 in charges on the 149 firm fixed price and time and materials invoices that it reviewed were adequately supported, allowable under the terms

and conditions of the contract and task orders, and properly allocated to their respective task orders. In addition, the contractor determined that Lockheed had allocated the remaining $339,794,230 in firm fixed price and time and materials charges invoiced during the period covered by the audit to the correct task orders. The contractor also identified an additional $4,046 in unallowable travel agent booking fees, resulting in total questioned costs of $4,170, which we have reported in our Semiannual Report to the Congress.

We have a number of ongoing or planned assignments designed to address other aspects of the Corporation's business activities. Among those are assignments in the following areas:

- **The FDIC's Controls Over IT Hardware Asset Management:** The assignment objective is to evaluate to what extent the FDIC has established key controls to mitigate risks associated with the FDIC's IT hardware asset management program.
- **FDIC Non-Headquarters Facility Physical Security:** FDIC policy is to comply with a range of federal governing authorities intended to ensure that minimum physical security standards are maintained across federal agencies to safeguard employee, facilities, and operational missions. Our evaluation will seek to ensure that practices in place help protect the FDIC's personnel and physical resources in field locations.
- **DRR Hiring Practices:** We initiated an evaluation in response to three OIG hotline complaints that we received regarding DRR's hiring practices. The objective of this evaluation is to assess the merits of the complaints, while focusing on the hiring processes in place and possible improvements to those processes.

INVESTIGATION PRIORITIES AND RESULTS

Throughout FY 2017 and into FY 2018, our Office of Investigations will continue its efforts 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. These efforts are carried out by our criminal investigators, forensic and financial analysts, and investigators in our Electronic Crimes Unit. We are maintaining our close working relationships with law enforcement partners, including the Department of Justice; the Federal Bureau of Investigation; and other federal, state, and local law enforcement agencies. We are also coordinating closely with FDIC divisions and offices and other regulatory OIGs in conducting financial services investigations, both criminal and civil. The OIG also actively participates on numerous financial fraud, suspicious activity report, mortgage fraud, and other working groups nationwide to keep current with new threats and fraudulent schemes that can undermine the integrity of the FDIC's operations and the financial services industry as a whole. These include the Bank Fraud Working Group, Mortgage Fraud Working Group, Federal Financial Enforcement Task Force, all spearheaded by the Department of Justice.

The following cases are illustrative of recent OIG investigative success:

- The former president and chairman of First State Bank of Altus, Altus, Oklahoma, was sentenced to 48 months in prison after a jury convicted him in July 2016 of bank fraud, conspiracy to commit bank fraud, misapplication of bank funds, making a false bank entry, and unauthorized

issuance of a bank loan in connection with First State Bank of Altus, and various loan schemes. He was also ordered to pay $10,120,166.S8 in restitution to the FDIC.

- A former bank branch manager at First Tennessee Bank, N.A., Memphis, Tennessee, was sentenced to serve 36 months in federal prison for embezzlement of funds and tax evasion, to be followed by S years of supervised release. He was also ordered to pay restitution in the amounts of $844,254 to First Tennessee Bank, $161,018 to the Internal Revenue Service and $81,014 to two additional victims of his crimes, for a total of $1,086,286. Of the total amount he embezzled, the former bank manager obtained approximately $967,573 for his personal use.
- Two developers of the Indian Ridge Resort located in Branson, Missouri, were sentenced in the District of Kansas. They were each sentenced to serve 60 months in prison to be followed by 24 months of supervised release. The wife of one of developers was sentenced to 36 months of supervised release. On May 27, 201S, the three each entered guilty pleas for their role in a real estate construction fraud scheme charging them with bank fraud, conspiracy to commit bank fraud, money laundering, and conspiracy to commit money laundering.
- A businessman, the owner and president of Machine Tools Direct, Inc., was sentenced to serve 36 months in prison and was ordered to pay restitution of $97,331,250 for his role in a wire fraud scheme. He and a business partner were indicted on February 27, 2014, and charged with mail fraud, bank fraud, and wire fraud.
- A former vice president and Bank Secrecy Act officer of a Maryland bank pleaded guilty to wire fraud and bank embezzlement, arising from a 6-year scheme to steal over $1.8 million from bank customers at the bank where she worked. The former vice president admitted that she used her position of trust at the bank to cause more than 200 unauthorized transfers and withdrawals of funds from six customers' bank accounts to pay for mortgages, credit card bills, and property tax bills associated with her and her family members. Three of the six victim customers were at least 80 years old, and for two of the accounts, the customers were deceased.
- In one of our employee cases, a former senior capital markets specialist employed by the FDIC was sentenced to serve 2 years of probation in connection with his prior plea of guilty to a misdemeanor charge of intentionally exceeding authorized access to an FDIC computer to obtain information. Between January 2011 and September 2012, he emailed over 900 FDIC documents to his personal email account, including sensitive, confidential, and strictly private information regarding and belonging to systemically important financial institutions.

Dver the past year, we also continued to enhance our understanding and involvement in the IT security and cyber arena on multiple fronts, and in this regard, our Dffice of Investigations has played an important part. Our efforts include increasing our involvement with the FBI's Cyber Task Force in Washington D.C. and assigning one of our special agents to serve as our representative on the National Cyber Investigative Joint Task Force, a group focusing on cyber threat investigations across the federal, state, local, and international law enforcement, intelligence, counterintelligence, and military communities. A senior-level member of the Dffice of Investigations continued to closely monitor cyber-related activities at the FDIC and in the various external communities to help inform our work as an OIG. Finally, we have also participated in training activities sponsored by the 1st 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.

Our goal is to leverage the expertise and experience of our own staff, subject matter experts in other parts of the FDIC, and investigative entities external to the Corporation to more fully understand cyber-threats, respond as needed, and share information as we seek to protect the FDIC's and the nation's critical infrastructure.

Our current investigative caseload includes 294 open assignments, consisting of 268 investigations and 26 inquiries. Of the investigations, 187 relate to open bank matters, 47 to closed bank matters, and the remaining 34 cases relate to other potential criminal activity in the financial services sector. We anticipate that our FY 2017 and FY 2018 caseload will continue to include a large number of open and closed bank matters, sometimes involving fraud and other misconduct on the part of senior bank officials, money laundering, and mortgage and commercial loan fraud exposed by turmoil in the housing, commercial real estate, and lending industries. The remaining investigations would likely include cases involving misrepresentations of FDIC insurance or affiliation, cyber crimes, and a number of employee misconduct cases.

Another ongoing priority initiative involves coordinating with the FDIC Legal Division, Division of Risk Management Supervision, and DRR on matters related to enforcement actions. Specifically, we have established a program/schedule to share information to ensure that the OIG's investigative results are available to FDIC management in its consideration of civil and administrative enforcement activities, and that information developed by the FDIC is effectively communicated to OIG criminal investigators, when warranted. Finally, with regard to our criminal investigations, we are leveraging and strengthening our forensic accounting and financial analysis capabilities and continuing to explore was to be more proactive in identifying cases in areas where we have historically been more reactive in our approach. To that end, during FY 2017, we supplemented our investigative resources by hiring three financial analysts (for our New York, Dallas, and Chicago offices) to assist in the ongoing support of our open investigations. In addition, our financial analysts have represented our office on some of the task forces that we participate in and are taking a leading role in data analysis for new case leads.

MANAGEMENT PRIORITIES

We are continuing to examine our internal operations, workload, and human resource and IT needs. We are focusing particular attention on the OIG's IT environment to ensure it is secure and that our data are not compromised. As it relates to IT, the FDIC has decided to provide commodity services (such as email) in the cloud environment and is likely to move its entire IT operation to the cloud. The cloud environment presents significantly different operational, security, and management challenges for our office, and we will be developing a comprehensive plan to ensure our office's needs are met. Those needs may have a significant impact on our budget in FY 2018 and in future fiscal years. In the human resources area, in light of recent and future attrition in our office, we are focusing on succession planning. This focus has resulted in the addition of new staff at all levels and in various components of

our organization and changes in responsibilities for other staff, requiring flexibility on the part of all as we adjust to change.

CONCLUSION

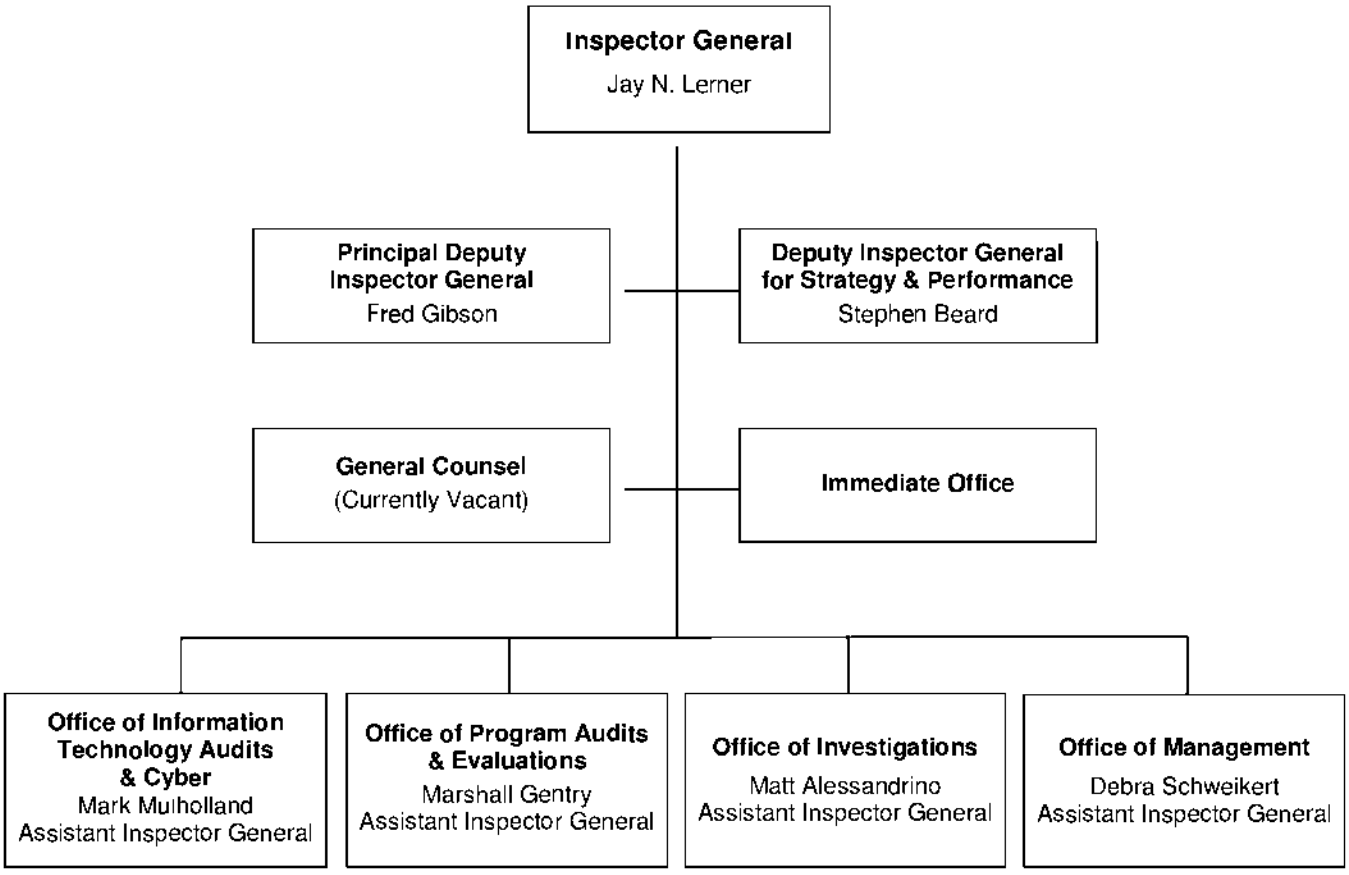
The FDIC OIG appreciates the support it has received from the Congress and the FDIC over the past years. Our work in FY 2018 will continue to build on our past and current efforts. We believe that our FY 2018 budget strikes an appropriate balance between the mandate of the IG Act, other legislative requirements, OIG workload and human resource needs, post-crisis challenges and risks facing the FDIC, and lingering uncertainties in the economy and financial services industry. The budgetary resources we have proposed reflect an increase over those we have operated with over the past fiscal years. We believe, with appropriate monitoring and a degree of flexibility, they will allow us to provide needed oversight to protect the government's and taxpayers' interests and to help sustain public trust and confidence in the nation's financial system. In the months ahead we will continue to monitor the risks to the FDIC's successful achievement of its mission and seek to ensure that our office will have and prudently manage the needed resources to fully carry out the oversight role entrusted to us under the IG Act. We proudly reaffirm our commitment to effectively and efficiently conduct work in service to the Congress, the FDIC, and the American public.

Appendix I

FDIC OIG Organization Structure and Office Descriptions

The structure of the FDIC OIG is based on the functional responsibilities legislated by the Inspector General Act of 1978 and with consideration to the FDIC's mission and operations. The FDIC OIG is comprised of the Inspector General's Immediate Office and component offices as shown below. We note that Mr. Jay N. Lerner became the FDIC Inspector General on January 9, 2017. 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 **General Counsel's Office** 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. Counsel also provides legal research and opinions; reviews audit, evaluation, and investigative reports for legal considerations; represents the OIG in personnel-related cases; leads Whistleblower Protection activities; coordinates the OIG's responses to requests and appeals made pursuant to the Freedom of Information Act and the Privacy Act; prepares IG subpoenas for issuance; reviews and comments on proposed or existing legislation; and coordinates with the FDIC Legal Division, as necessary.

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.

The **Office of Program Audits and Evaluations** conducts program evaluations and performance audits to assess how effectively FDIC is achieving its goals and objectives. This group also conducts reviews of failed banks and other systemic issues, and compliance audits.

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, and IT support; the OIG's internal and external Web sites; internal controls; coordination of OIG reviews of FDIC proposed policy and directives; and OIG policy development.

The **Office of Investigations** (OI) carries out a comprehensive nationwide program to prevent, detect, and investigate criminal or otherwise prohibited activity that may harm the operations or integrity of the FDIC and its programs. OI partners with the U.S. Department of Justice; the Federal Bureau of Investigation; other OIGs; and federal, state, and local law enforcement agencies. OI also coordinates closely with the FDIC's Division of Risk Management Supervision, Division of Resolutions and Receiverships, and the Legal Division in investigations involving open and closed institutions. OI operates an Electronic Crimes Unit and forensic laboratory. OI also manages the OIG Hotline for employees, contractors, and others to report instances of suspected fraud, waste, abuse, and mismanagement within the FDIC and its contractor operations via a toll-free number, e-mail, or regular mail.

Appendix II

FY 2016 Accomplishments

In FY 2016, results of OIG audits, evaluations, and investigations were as follows:

Significant Outcomes (October 1, 2015 –September 30, 2016)	
Audit and Evaluation Reports Issued	12
Questioned Costs or Funds Put to Better Use	$55,000
Nonmonetary Recommendations	28
Investigations Opened	104
Investigations Closed	90
OIG Subpoenas Issued	23
Judicial Actions:	
Indictments/Informations	75
Convictions	76
Arrests	38
OIG Investigations Resulted in:	
Fines of	$99,521
Restitution of	1,096,575,046
Asset Forfeitures of	1,185,757
Total	**$1,097,860,324**
Cases Referred to the Department of Justice (U.S. Attorney)	73
Proposed Regulations and Legislation Reviewed	16
Responses to Requests Under the Freedom of Information/Privacy Act	20

Appendix III

FY 2018 Appropriation Bill Language, Object Classification, and Personnel Summary*

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, $39,136,000 to be derived from the Deposit Insurance Fund.

Object Classification	FY 2016 Actual (000 omitted)	FY 2017 Budget (000 omitted)	FY 2018 Proposed (000 omitted)
11.1 Full-Time Equivalent	$19,176	$22,077	$22,858
11.5 Other Personnel Compensation	844	872	1,000
11.9 Total Personnel Compensation	$20,020	$22,949	$23,858
12.0 Civilian Personnel Benefits	8,816	9,488	10,473
21.0 Travel and Transportation of Persons	1,177	1,340	1,595
22.0 Transportation of Things	28	28	28
24.0 Printing and Reproduction	0	0	0
25.0 Other Services**	2,746	1,618	2,197
26.0 Supplies and Materials	18	10	15
31.0 Equipment	143	525	970
Total Appropriation	**$32,948**	**$35,958**	**$39,136**

Personnel Summary	FY 2016 Actual	FY 2017 Budget	FY 2018 Proposed
Total Compensable Work Years:			
Full-Time Equivalent Employment	119	137	144
Full-Time Equivalent Interns	1	1	1
Full-Time Equivalent Overtime and Holiday	1	1	1

* The FDIC OIG receives a lump-sum appropriation for "necessary expenses of the Office of Inspector General in carrying out the provisions of the Inspector General Act of 1978." This Appendix represents the FDIC OIG's best estimate of our needs during the appropriations period, but the OIG may modify specific allocations, as needed.

** Other Services in FY 2018 includes $250,000 for training and $78,000 for support of the Council of the Inspectors General on Integrity and Efficiency.