Budget for Fiscal Year 2021

February 2020

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation
Office of Inspector General

TABLE OF CONTENTS

OFFICE OF INSPECTOR GENERAL BUDGET FOR FY 2021

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) presents its proposed budget for Fiscal Year (FY) 2021. In this document, we will present the following information:

- Mission and Vision
- Source of OIG Funding
- Proposed Fiscal Year 2021 Budget
- OIG Accomplishments in Fiscal Year 2019
    - Audit and Evaluation Reports
    - Results of OIG Investigations
- Top Challenges Facing the FDIC

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 $7.7 trillion in deposits at approximately 5,250 banks and savings associations and directly supervises about 3,380 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 does not receive any Congressional appropriation; the agency is funded by premiums that banks and thrift institutions pay for deposit insurance coverage and earnings on investments in U.S. Treasury securities.

The FDIC Office of Inspector General is an independent organization established under the Inspector General (IG) 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 FDIC 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 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 created the Financial Stability Oversight Council and further established the Council of Inspectors General on Financial Oversight (CIGFO). This Council facilitates sharing of information among CIGFO member Inspectors General, confers on issues that relate to the financial sector, and considers ways to improve financial oversight.

In addition, we meet with representatives of the Government Accountability Office (GAO) to coordinate work efforts. We also collaborate with our law enforcement partners, including the Department of Justice (Federal Bureau of Investigation and U.S. Attorneys' Offices) and other OIGs.

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 failed institution. Also, the FDIC OIG annually conducts a review of the agency's information security program and practices pursuant to the Federal Information Security Modernization Act of 2014 (FISMA) and, bi-annually, pursuant to the Digital Accountability and Transparency Act of 2014 (DATA).

Appendix I presents an overview of the FDIC OIG's current organizational structure and a brief description of our component divisions. Appendix II presents statistics on OIG productivity in FY 2019. Appendix III presents our budget request for FY 2021.

SOURCE OF OIG FUNDING

The FDIC OIG derives its spending authority from two sources: the Federal Deposit Insurance Act (FDI Act) and annual appropriations acts. The FDI Act provides permanent authority for the FDIC to fund its operations from the DIF without further appropriation, and this was the sole authority for OIG funding from its establishment in 1989 through FY 1997. Beginning in FY 1998, in order to promote the independence of the OIG, the Congress has specified in annual appropriations acts the amount from the DIF that is to be allocated to the OIG for the OIG's exclusive use. Although the amount of funding is specified in the appropriations act, the acts have also specified that the source of the funding remains the DIF created by the FDI Act, not the Treasury. Through its annual budget process as authorized by the FDI Act, at the beginning of each calendar year the FDIC allocates from the DIF to the OIG an amount calculated by estimating the amount to be specified in appropriations, and later adjusts that allocation if enacted appropriations specify an amount different than the estimate.

PROPOSED FISCAL YEAR 2021 BUDGET

The FDIC OIG's proposed FY 2021 budget is approximately $43 million. Of this amount, approximately $35.6 million (83 percent) is allocated to personnel costs, including benefits. The remaining $7.4 million (17 percent) includes information technology (IT) expenditures, travel costs, contract-related expenses, and contributions to the Council of the Inspectors General on Integrity and Efficiency.

We intend to fill existing vacancies throughout FY 2020 and into FY 2021 in order to address recent retirements and anticipated attrition, and to supplement our current needs. In particular, we will be hiring personnel with competencies appropriate for evaluating the FDIC's efforts in addressing management and performance challenges, including emerging cyber security risks. We also intend to sustain focus on enhancing our capability to examine cybercrime cases related to the banking sector.

In addition, we will continue to enhance the OIG's internal IT needs. The OIG is taking a strategic approach to refresh and enhance its IT environment to improve flexibility, scalability, and resiliency of the OIG's IT capabilities. Our FY 2021 budget includes funding for equipment, software, licenses, and contractual services that enable us to maintain and modernize our IT infrastructure, business applications, and Electronic Crimes Unit. Our FY 2021 budget also provides funding for contractor services to sustain internal operations efficiently.

Additional details regarding our budget request for FY 2021 are presented in Appendix III.

OIG ACCOMPLISHMENTS IN FISCAL YEAR 2019

A top priority for the FDIC OIG in FY 2019 was modernizing and integrating technology in OIG processes, and ensuring operations and controls are consistent with applicable requirements, professional standards, and best practices. To that end, we completed transitioning OIG email to the cloud and continued our preparation for migration to Microsoft Office 365. We also completed important steps for our IT refresh, including needed hardware and software, effective backup capabilities and processes, and development of an architecture project plan. In addition, we made substantial progress in improving the operations and procedures of the OIG's Electronic Crimes Unit Laboratory for computer forensics in criminal cases.

We also undertook several initiatives to improve the efficiency and effectiveness of our Office. We leveraged our data analytics capabilities to improve our audit and evaluation assignments; identify fraud, waste, and abuse; and facilitate OIG decision-making. We reviewed and revised our emergency planning to address changes in the organization, business needs, and relevant government-wide standards and best practices. We also continued to review and update a number of OIG internal policies and delegations of authority related to audits, evaluations,

investigations, management operations, and administrative processes to ensure that they provided the basis for quality work.

We also continued to focus on the long-term preparedness and success of the OIG. To that end, we filled key positions, including the Deputy Inspector General, a vacancy created through attrition. We continue to focus on hiring personnel to enhance skills and experience within the Office. We also recognize the importance of employee engagement in the workplace, and established a new Workforce Council comprised of volunteer non-supervisory staff members representing a cross-section of the OIG. The areas of responsibility of the Council include employee-driven leadership, promoting collaboration and innovation, and analyzing employee-focused initiatives. The OIG also continued its Diversity and Inclusiveness Working Group to foster a sense of teamwork and mutual respect across the workplace.

The OIG recognizes the importance of transparency in these initiatives and all OIG work. We continued to focus on keeping the American public informed through:

- The FDIC OIG website, www.fdicoig.gov, which includes summaries of completed work, a listing of ongoing work, and information on unimplemented recommendations;
- Twitter communications that immediately disseminate news of note; and
- Participation in the IG community's oversight.gov website, which enables users to access thousands of previously-issued IG reports and other oversight areas of interest.

We also maintained our OIG Hotline to field complaints and other inquiries from the public and stakeholders, and our Whistleblower Protection Coordinator educated FDIC employees on their rights and remedies against retaliation for making protected disclosures. We look forward to continuing these and other outreach efforts.

Audit and Evaluation Reports

During FY 2019, we issued eight audit and evaluation reports and made 50 recommendations to strengthen controls in FDIC programs and operations. Our completed and on-going work covered diverse topics such as information technology and cybersecurity, physical security of FDIC facilities, contract management oversight, crisis readiness, minority depository institutions, and the FDIC's cost benefit analysis process for rulemaking.

The following summaries highlight the findings from five of the eight completed audit and evaluation reviews during FY 2019.

The FDIC's Physical Security Risk Management Process

This evaluation determined the extent to which the FDIC's physical security risk management process met Federal standards and guidelines.

The FDIC employs approximately 6,000 individuals and has about 3,000 contractor personnel who conduct their work at 94 FDIC-owned or leased facilities throughout the country. FDIC facilities house highly sensitive banking and personally identifiable information, mission-critical systems, and valuable equipment. The FDIC must ensure its employees, contractors, resources, and assets are safe and secure.

In 1995, the President issued an Executive Order which created the Interagency Security Committee (ISC). This Committee has issued Government-wide standards, policies, and best practices applicable to all buildings and facilities occupied by Federal employees for non-military activities. The ISC standards provide a structured methodology for helping to ensure the safety of employees, contractors, and facilities by assessing facility risk, assigning facility security levels, and determining whether implemented countermeasures effectively mitigate risk. The FDIC adopted the recommended minimum security standards issued by the ISC for all FDIC facilities where practical.

Our evaluation determined that the FDIC had not established an effective physical security risk management process to ensure that it met ISC standards and guidelines. While FDIC management has indicated that there have been no major incidents or threats to any FDIC facility over the past 10 years, we found that the FDIC's physical security risk management process needed improvement:

- The FDIC had not developed adequate policies and procedures, quality control standards, training requirements, or record keeping standards. FDIC officials responsible for the Physical Security Program had not emphasized compliance with the ISC standards, and instead placed priority attention on other security initiatives.

- The FDIC did not conduct key activities in a timely and thorough manner for determining facility risk level, assessing security protections in the form of countermeasures, and mitigating and accepting risk.

- The FDIC did not adequately address countermeasures or track recommendations for minimum security protections. At some facilities, these countermeasures remained outstanding for more than 4 years, and in some cases, the FDIC could not provide the resolution status of recommendations.

- In certain instances, the FDIC was not able to provide justification for significant expenditures for countermeasures beyond recommended security protections.

- The FDIC had not developed goals and performance measures to help ensure its physical security program was effective.

Our evaluation did not assess the safety of FDIC personnel and its facilities. Nevertheless, without a more robust physical security risk management process, the FDIC could not be certain

that it had taken appropriate and cost-effective measures commensurate with risk and aligned with ISC standards.

We made nine recommendations to address the weaknesses in the FDIC's physical security risk management process; the FDIC concurred with these recommendations. We believe that the planned corrective actions are significant undertakings by the Agency and, once implemented, are likely to achieve important improvements towards the efficiency and effectiveness of its risk management process for physical security.

Preventing and Detecting Cyber Threats

In this audit, we assessed the effectiveness of two security controls intended to prevent and detect cyber threats on the FDIC's network: Firewalls; and the Security Information and Event Management (SIEM) tool. The FDIC's firewalls and SIEM tool operate in concert with other network security controls as part of a defense-in-depth cybersecurity strategy.

The FDIC has deployed firewalls at the perimeter and interior of its network to control the flow of information into, within, and out of the network. These network firewalls use rules to enforce what traffic is permitted. The FDIC's SIEM tool operates to analyze network activity and detect indications of potential cyber threats that may have bypassed the firewalls and other security controls. The tool runs automated queries (known as "Use Cases") to identify events or patterns of activity that may indicate a cyber attack.

We identified weaknesses that limited the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats, including:

- The majority of firewall rules were unnecessary. Also, many firewall rules did not have sufficient justification. Several factors contributed to these weaknesses, including an inadequate firewall policy and supporting procedures, and an ineffective process for periodically reviewing firewall rules to ensure their continued need.

- Firewalls did not comply with the FDIC's minimally acceptable system configuration requirements. In addition, the FDIC did not update its minimum configuration requirements in a timely manner to address new security configuration recommendations by the National Institute of Standards and Technology.

- The FDIC did not always require administrators to uniquely identify and authenticate when they accessed network firewalls.

We found that the FDIC properly set up the SIEM tool to collect audit log data from key network IT devices. In addition, the SIEM tool effectively formatted the data to allow for analysis of potential cyber threats. However, the FDIC did not have a written process to manage the ongoing identification, development, implementation, maintenance, and retirement of Use Cases for the SIEM tool.

We made 10 recommendations intended to strengthen the effectiveness of the FDIC's network firewalls and SIEM tool in preventing and detecting cyber threats. The FDIC concurred with our recommendations.

Minority Depository Institution Program at the FDIC

This evaluation reviewed the FDIC's Minority Depository Institution (MDI) Program. Minority Depository Institutions play a vital role in assisting minority and under-served communities and are resources to foster the economic viability of these communities.

The FDIC considers an institution to be an MDI if it is a Federally-insured depository institution where a majority of a bank's voting stock is owned by minority individuals; or a majority of the institution's Board of Directors is minority and the institution serves is a predominantly minority community.

The Financial Institutions Reform, Recovery, and Enforcement Act (FIRREA) of 1989 required the FDIC to consult with the Secretary of the Treasury on methods for best achieving five statutory goals aimed at preserving and promoting MDIs. In keeping with the requirements of FIRREA, the FDIC adopted an MDI Policy Statement describing its interpretation of ways to preserve and promote MDIs and implement the goals.

We concluded that the FDIC achieved its program goals as outlined in the MDI Policy Statement. That is, the FDIC took actions to preserve and promote MDIs, and preserve the minority character of MDIs; provided technical assistance to MDIs; encouraged the creation of new MDIs; and provided MDI training sessions, education, and outreach efforts. Notwithstanding these efforts, we found that the FDIC did not evaluate the effectiveness of key MDI Program activities. Specifically, the FDIC did not assess the effectiveness of its supervisory strategies and MDI technical assistance. We also determined that the FDIC should further assess the effectiveness of its MDI training sessions, education, and outreach, including the benefit and value that they provide.

The FDIC also did not define the types of activities that it considered to be MDI technical assistance, as distinct from training, education, and outreach events. Additionally, while the FDIC provided training, education, and outreach events, the MDI banks, FDIC Regional Coordinators for MDIs, and representatives from MDI trade associations requested that the FDIC provide more such events.

Our report contained five recommendations to improve the FDIC's MDI Program. FDIC management concurred with the recommendations.

The FDIC's Information Security Program–2018

We issued our report on the *FDIC's Information Security Program—2018* and contracted with Cotton & Company (C&C) LLP to perform this audit. C&C identified 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.

Information Security Risk Management: The FDIC had not fully defined or implemented an enterprise-wide and integrated approach to identifying, assessing, and addressing the full spectrum of internal and external risks, including those related to cybersecurity and the operation of information systems. The FDIC did not have an approved risk appetite, risk tolerance level, and risk profile, which limited effective risk management decision-making. Further, the FDIC cannot be sure that it is effectively prioritizing resources toward addressing risks with significant potential impact on achieving strategic objectives.

Enterprise Security Architecture: Our FISMA audit report in 2017 noted that the FDIC had not established a fundamental component of an effective information security program—an enterprise security architecture. The lack of an effective enterprise security architecture increased the risk that the FDIC's information systems would be developed with inconsistent security controls that are costly to maintain. In June 2018, the FDIC completed an enterprise security architecture document; we plan to evaluate whether this document is responsive to our earlier concerns.

Security Control Assessments: Based on separate OIG audit work, discussed later in this document, the OIG identified instances in which contractor-performed security control assessments did not include testing of security control implementation, when warranted. Instead, assessors relied on narrative descriptions of the controls in FDIC policies, procedures, and system security plans and interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls. The FDIC must ensure that personnel perform security control assessments at an appropriate level of depth and coverage.

Patch Management: The FDIC's patch management processes were not always effective in ensuring that the FDIC implemented patches within FDIC-defined timeframes. In addition, the FDIC had not developed and implemented an effective process to ensure that vulnerabilities resulting from patches that have not been installed within required timeframes were tracked and reported to senior management. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.

Backup and Recovery: The FDIC had limited assurance that it could maintain and restore mission-essential functions during an emergency within applicable timeframes, until scheduled completion of its backup data center. In December 2017, the FDIC's Board of Directors authorized a multi-year project designed to ensure that designated IT systems and applications

supporting mission-essential functions could be recovered within targeted timeframes. As part of this project, the FDIC planned to migrate key IT systems and applications to a new and expanded backup data center in a different geographic location.

We made four recommendations to improve the effectiveness of the FDIC's information security program controls and practices. FDIC management concurred with these recommendations. The FDIC was also working to implement an additional nine recommendations from prior FISMA audit reports.

Security Configuration Management of the Windows Server Operating System

Our audit focused on the FDIC's controls for managing security configurations and changes to its Microsoft Windows Server operating system. At the start of 2018, the FDIC had 2,166 servers on its network running the Microsoft Windows Server operating system. These servers store and process a significant volume of sensitive information and support mission-critical functions.

Federal agencies are required by statute to comply with certain system configuration requirements. Without effective configuration management, information systems may not operate properly, stop operating altogether, or become vulnerable to security threats. The objective of the audit was to determine whether the FDIC established and implemented controls for managing changes to its Windows Server operating system that were consistent with Federal requirements and guidelines.

The FDIC established various controls to manage changes to its Windows Server operating system, including an approved baseline configuration for the operating system; a system to track and report system changes; and a governance body to evaluate proposed changes. These controls were consistent with Federal requirements and applicable guidelines.

However, we found several deficiencies in the FDIC's management of security configurations for its Windows servers:

- The FDIC did not establish current policies and procedures for managing changes to the Windows Server operating system. Accordingly, we did not have sufficient criteria to fully assess the FDIC's implementation of configuration management controls.

- The FDIC hired a contractor firm to assess certain security controls, including configuration management controls, for which the FDIC had also assigned the firm duties related to design and/or execution. Tasking this firm with assessing the effectiveness of its own work affected the independence of such assessments.

- FDIC oversight activities were inadequate in identifying instances in which security control assessors did not perform actual testing of certain security controls, when appropriate, including those intended to protect the Windows Server operating system.

In these cases, when concluding on control effectiveness, assessors relied solely on written descriptions of the controls in FDIC policies, procedures, and system security plans and/or interviews of FDIC or contractor personnel.

- The security plan for the Windows Server operating system contained several inaccurate descriptions of security controls.

Our report included eight recommendations to address the concerns we identified. The FDIC concurred with the recommendations.

Results of OIG Investigations

The FDIC OIG's Office of Investigations aims to preserve the integrity of the FDIC and banking system. Our Office of Investigations works to prevent, detect, and investigate criminal or otherwise prohibited activity that may threaten to harm the operations or integrity of the FDIC and the banking sector.

Our investigations are largely based upon referrals from the FDIC; our law enforcement partners, including other Offices of Inspector General; and the Department of Justice, including U.S. Attorneys' Offices and the Federal Bureau of Investigation. Our relationships with law enforcement partners have led to key roles in investigating sophisticated schemes of bank fraud, money laundering, embezzlement, and currency exchange rate manipulation. These cases often involve bank executives, officers, and directors, as well as other financial insiders such as attorneys, accountants, and commercial investors.

A recent area of focus for our investigations has been partnering with other regulatory agencies to identify fraud in the guaranteed loan portfolios of FDIC-supervised banks. Such large-scale fraud schemes can affect the financial condition of banks and the financial services industry. In addition, we aim to be proactive in our investigative work by identifying and assessing emerging issues affecting the FDIC and the banking sector. We anticipate that our role in combating cyber-related financial fraud will increase this year, and we have augmented our resources to address such crimes.

During FY 2019, FDIC OIG investigations resulted in 77 indictments and informations; 61 convictions; 34 arrests; and fines, restitution ordered, and asset forfeitures exceeding $445.9 million. The following cases are illustrative of these OIG investigative accomplishments, achieved through collaborative efforts with Federal, state, and local law enforcement entities.

South Florida Resident Convicted and Sentenced for a $100 Million International Fraud Scheme That Led to the Collapse of One of Puerto Rico's Largest Banks

On February 4, 2019, Jack Kachkar, former Chief Executive Officer and Chairman of now bankrupt Inyx Inc., a multinational pharmaceutical company, was convicted of eight counts of wire fraud affecting a financial institution after a 3-week trial in the Southern District of Florida.

Kachkar was sentenced on July 2, 2019, to 30 years in prison, followed by 5 years of supervised release for his role in a $100 million scheme to defraud Westernbank of Puerto Rico. The losses from the scheme led to the eventual insolvency and collapse of Westernbank. Kachkar was also ordered to pay $103,490,005 in restitution to the FDIC, as receiver for Westernbank.

According to evidence presented at trial, from 2005 to 2007, Kachkar served as chairman and chief executive officer (CEO) of Inyx, Inc., a publicly-traded multinational pharmaceutical manufacturing company. Beginning in early 2005, he caused Westernbank to enter into a series of loan agreements in exchange for a security interest in Inyx's assets. Under the loan agreements, Westernbank agreed to advance money based on Inyx's customer invoices from "actual and bona fide" sales.

However, Kachkar orchestrated a scheme to defraud Westernbank by causing numerous Inyx employees to make tens of millions of dollars' worth of fake customer invoices purportedly payable by customers in the United Kingdom, Sweden, and elsewhere. He caused these invoices to be presented to Westernbank as valid invoices and made false representations to Westernbank about purported repayments from lenders in order to lull Westernbank into continuing to lend money to Inyx. He also fraudulently represented to Westernbank executives that he had additional collateral, including purported mines in Mexico and Canada worth hundreds of millions of dollars, to induce Westernbank to lend additional funds.

Kachkar caused Westernbank to lend approximately $142 million and diverted tens of millions of dollars for his own personal benefit, including to buy a private jet, luxury homes and cars, luxury hotel stays, and extravagant jewelry and clothing expenditures.

In or around June 2007, Westernbank declared the loan in default and ultimately suffered losses exceeding $100 million. These losses later triggered a series of events leading to Westernbank's insolvency and ultimate collapse. At the time of its collapse, Westernbank had approximately 1,500 employees and was one of the largest banks in Puerto Rico.

In addition, Kachkar knowingly deposited a $3 million check at Mellon Bank from the purported sale of his private jet. At the time of its deposit, he knew that the check was worthless – he had actually agreed to sell his plane to a different buyer. After receiving a provisional credit for the check from Mellon Bank, he wired out all of the provisional credit, including a $1 million wire to his personal account in Canada. Upon Mellon Bank's request to reverse this $1 million wire, Kachkar refused to do so, resulting in at least a $1 million loss to Mellon Bank.

Former Bank President Sentenced to Prison and Ordered to Pay $137 Million

On December 14, 2018, John A. Shelley, the former president and CEO of The Bank of Union in El Reno, Oklahoma, was sentenced to 4 years in federal prison followed by 2 years of supervised release for making a false statement to the FDIC. He had previously pleaded guilty to this charge in 2017. The sentence requires the former president to pay over $137 million in

restitution, over $97 million of which is owed to the FDIC. State banking regulators closed The Bank of Union in 2014 because of the bank's loan losses, and the FDIC was appointed as receiver.

According to a 2016 indictment, Shelley defrauded the bank in several ways: (1) issuing loans with insufficient collateral and falsifying financial statements for several high-dollar bank borrowers; (2) originating nominee loans to circumvent the bank's legal lending limit; (3) concealing the bank's true financial condition from the Board of Directors; (4) soliciting a fraudulent investment; and (5) falsely representing the bank's true status to the FDIC.

Over a 4-year period, Shelley conspired with borrowers by issuing them millions of dollars in loans secured by collateral they did not have and issuing them new loans to keep them off of overdraft reports. He misled the bank's Board of Directors by falsely stating the borrowers were paying down their loans.

Shelley also defrauded a partial owner and investor in the bank by convincing him to wire nearly $40 million. He falsely represented to the investor that the bank was growing rapidly and performing well and that his investment would not be at risk, despite knowing that the bank was on the brink of failure and needed an immediate capital infusion.

Finally, Shelley was charged with falsely representing the bank's loan status to the FDIC. Between September 2012 and September 2013, he continued to renew certain unpaid loans by capitalizing unpaid interest. Pursuant to a 2013 FDIC examination, he allegedly falsely represented that he had not renewed or extended any loans without full collection of the interest due during that time period. He also falsely represented in writing that the bank had total equity capital of more than $36 million in July 2013, when he knew the bank's equity capital was significantly less.

The partial owner who wired money for the bank's benefit was due $40 million of the restitution amount, and the remaining $97 million was due to the FDIC, which lost money when it assumed the bank's liabilities as receiver in January 2014.

Investment Advisor Sentenced to 262 Months' Imprisonment for Multi-Million Dollar Investment Fraud Scheme and Income Tax Evasion

On August 29, 2019, Treyton Thomas was sentenced to 262 months' imprisonment for wire fraud and 60 months' imprisonment for income tax evasion, to run concurrently.

Thomas was first charged with 21 counts of wire fraud, bank fraud, and money laundering in 2016, when it was discovered that he defrauded his father's used car warranty company, NC & VA Warranty of Roxboro, N.C.; several of its customers; his wife; and his father-in-law. Through the use of an online brokerage firm, he used the defrauded funds to conduct risky trades in the commodities and futures market and then concealed the scheme by providing victims and financial institutions with sales information and fabricated bank and brokerage statements. To

obtain additional funds, Thomas then used the same false information and statements to defraud financial institutions out of $1.9 million in loan proceeds. He also spent more than $1.6 million to pay personal expenses.

In 2018, Thomas was then charged with six counts of income tax evasion for the calendar years 2010-2015 and two counts of failing to disclose his interest in and authority over foreign bank accounts. According to court evidence, the defendant failed to file income tax returns or pay taxes for 20 years, and concealed his income through offshore entities in the Cayman Islands, British Virgin Islands, and Nevis. He also had employees from offshore corporation management companies act as his nominee in multiple business ventures. In addition, Thomas created "ghost" employees to make it seem as though he operated a large, successful investment fund. He used aliases or variations of his own name to conceal his identity.

He was ordered to pay approximately $7.3 million in restitution to the victims of the schemes, the Internal Revenue Service, and the U.S. Attorney's Office. Additionally, he had to forfeit $7.3 million to the United States.

Ex-Bank Executive Sentenced to More than 5 Years in Prison for Loan Fraud

On May 20, 2019, the former chief marketing officer at the now-failed Mirae Bank was sentenced to 70 months in federal prison and ordered to pay $7,519,084 for his role in a scheme that caused Mirae Bank to issue more than $15 million in fraudulent loans.

From 2005 until 2007, Ataollah Aminpour represented himself as a successful business man who could help people obtain financing for gas station and car wash businesses. He used his role as a senior bank executive to submit and cause others to submit false information about the true purchase price of the business and also about the assets of the borrowers and the finances of the business that was purchased.

Aminpour also had the borrowers transfer money into escrow accounts so that it would falsely appear to the bank that borrowers were making large down payments. This allowed borrowers to acquire businesses with little to no money down and allowed Aminpour to earn commissions and misappropriate the excess loan proceeds for himself. Aminpour admitted that six different loan applications with false statements, totaling $16.7 million, were submitted between 2005 and 2007.

According to court documents, Aminpour also referred about $150 million in loans to Mirae Bank, and those loans largely contributed to the bank's collapse in 2009.

The FDIC and Wilshire Bank, which acquired Mirae's assets after its collapse, suffered more than $33 million in losses combined as a result of the ex-bank executive's scheme.

Our Office is committed to continuing its investigative activities to help preserve the integrity of the Agency and the financial system, and to protect depositors and financial consumers.

TOP CHALLENGES FACING THE FDIC

As required by statute, we identify the Top Management and Performance Challenges facing the FDIC. We conduct 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.

Last year, we identified nine areas representing the most significant challenges for the FDIC. We noted that these challenges would require constant attention and vigilance by the FDIC for the foreseeable future. As noted in our FY 2020 budget justification, we identified the following challenges:

- Enhancing Oversight of Banks' Cybersecurity Risk;
- Adapting to Financial Technology Innovation;
- Strengthening FDIC Information Security Management;
- Preparing for Crises;
- Maturing Enterprise Risk Management;
- Sharing Threat Information with Banks and Examiners;
- Managing Human Capital;
- Administering the Acquisitions Process; and
- Improving Measurement of Regulatory Costs and Benefits.

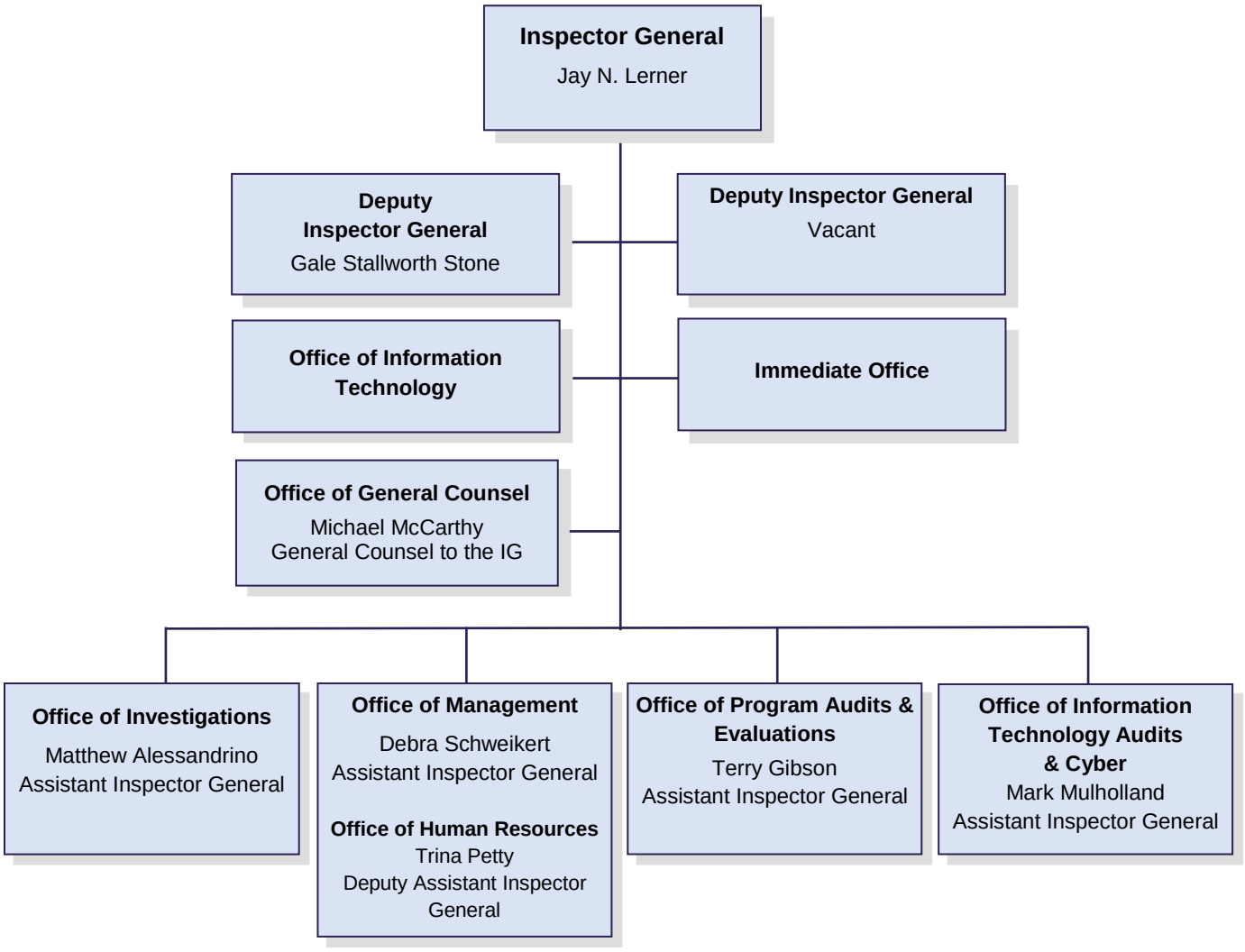
Our work during FY 2019 addressed a number of these challenges. We have updated our assessment of the challenges currently facing the FDIC and will be issuing our report on those challenges in mid-February 2020.

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 funding for FY 2021, 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 2021 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.

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



Regional 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 outreach, 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, and conducts investigations involving open and closed banks. 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, OIG websites, contracting and acquisition, records retention, internal controls, and OIG policies and directives.

The **Office of Human Resources** provides personnel support for the OIG in areas including recruitment, hiring, benefits, time and attendance, employee relations, and retirement.

The **Office of Information Technology** provides IT support for the OIG, including system development, access control, and security and privacy considerations.

In FY 2019, results of OIG audits, evaluations, and investigations were as follows:

Significant Outcomes (October 1, 2018 –September 30, 2019)	
Audit and Evaluation Reports Issued	8
Other Products Issued	5
Recommendations	50
Investigations Opened	67
Investigations Closed	79
Judicial Actions:	
Indictments/Informations	77
Convictions	61
Arrests	34
OIG Investigative Results:	
Fines	$56,500
Restitution Ordered	435,189,763
Asset Forfeitures	10,614,750
Total	**$445,861,013**

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 or, only when appropriate, the FSLIC Resolution Fund.			
Object Classification	**FY 2019 Actual (000 omitted)**	**FY 2020 Budget (000 omitted)**	**FY 2021 Proposed (000 omitted)**
11.1 Full-Time Equivalent *	$21,186	$24,941	$23,877
11.5 Other Personnel Compensation	803	850	825
11.9 Total Personnel Compensation	$21,989	$25,791	$24,702
12.0 Civilian Personnel Benefits	9,902	11,841	10,895
21.0 Travel and Transportation of Persons	1,165	975	1,228
22.0 Transportation of Things	28	14	14
25.0 Other Services **	3,013	2,754	3,865
26.0 Supplies and Materials	11	15	15
31.0 Equipment	626	1,592	2,263
Total Appropriation	**$36,734**	**$42,982**	**$42,982**

*The FDIC OIG follows the FDIC's compensation agreement; the FY 2021 budget request incorporates the estimated pay adjustment.

**Other Services in FY 2021 includes $555,000 for training and $115,000 for support of the Council of the Inspectors General on Integrity and Efficiency.