Budget for Fiscal Year 2020

March 2019

☆☆☆☆☆☆☆☆

Federal Deposit Insurance Corporation
Office of Inspector General

TABLE OF CONTENTS

OFFICE OF INSPECTOR GENERAL BUDGET FOR FY 2020

The Federal Deposit Insurance Corporation (FDIC) Office of Inspector General (OIG) presents its proposed budget for Fiscal Year (FY) 2020. In this document, we will present the following information:

- Mission and Vision
- Source of OIG Funding
- Proposed Fiscal Year 2020 Budget
- OIG Accomplishments in Fiscal Year 2018
    - Audit and Evaluation Reports
    - Special Inquiry Report
    - 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 $7.3 trillion in deposits at approximately 5,400 banks and savings associations and directly supervises about 3,500 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 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 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).

Appendix I presents an overview of the FDIC OIG's current organizational structure and a brief description of our component divisions. Appendix II presents a brief summary of the FDIC OIG's accomplishments in FY 2018. Appendix III presents our budget request for FY 2020.

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 2020 BUDGET

The FDIC OIG's proposed FY 2020 budget is approximately $43 million. Of this amount, approximately $37.5 million (87 percent) is allocated to personnel costs, including benefits. The remaining $5.5 million (13 percent) includes information technology (IT) expenditures, travel costs, contract-related expenses, and contributions to the Council of the Inspectors General on Integrity and Efficiency. The budget supports an authorized staffing level of 144, reflecting no change from FY 2019.

We intend to fill existing vacancies throughout FY 2019 and into FY 2020 in order to address recent retirements and anticipated attrition, and to supplement our current needs. In particular, we will be hiring personnel to supplement expertise in IT and information security so that we can improve identification and mitigation of emerging cybersecurity risks. We also plan to increase investigative personnel with requisite capabilities and experience for examining 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 2020 budget includes funding for equipment, software, licenses, and contractual services that enable us to maintain our IT infrastructure, business applications, and Electronic Crimes Unit (ECU). Our FY 2020 budget also provides funding for contractor services to sustain internal operations efficiently.

Appendix III presents our budget request for FY 2020.

OIG ACCOMPLISHMENTS IN FISCAL YEAR 2018

A top priority for the FDIC OIG in FY 2018 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 made significant progress in 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 initiated a review and revision of 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 Assistant Inspector General for Program Audits and Evaluations, Director for the Office of Information Technology, and Special Agent in Charge of the ECU. 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 supported the efforts of the IG Advisory Council – a cross-cutting group of OIG staff whose mission is to provide leadership towards "One OIG" by promoting collaboration and innovation. The OIG also established a 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, 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 2018, we issued eight audit and evaluation reports and made 49 recommendations to strengthen controls in FDIC programs and operations. Our work covered diverse topics such as information security, IT governance, compliance with the Digital Accountability and Transparency Act of 2014, functionality of a mission-critical FDIC system, processing of consumer complaints, and various FDIC supervision and consumer protection programs. The following summaries highlight the findings from several recently completed FDIC OIG audit and evaluation reviews.

The FDIC's Governance of Information Technology Initiatives

This audit report highlighted challenges and risks facing the FDIC with respect to the governance of its IT initiatives. The audit focused on key components of the FDIC's IT strategic planning, enterprise architecture, and governance bodies and practices. We reviewed these components in light of three IT initiatives: (1) migration of FDIC email operations to the cloud;

(2) deployment of laptop computers to FDIC employees and contractor personnel; and (3) proposed adoption of a managed services solution for mobile IT devices.

We reported that the FDIC faced a number of challenges and risks with respect to the governance of its IT initiatives. Although the FDIC had planned to develop an enterprise cloud strategy in 2017, it had not done so prior to pursuing cloud initiatives. Specifically, the FDIC had not fully developed a strategy to migrate IT services and applications to the cloud prior to executing initiatives, nor had the FDIC obtained the acceptance of organizational stakeholders across the FDIC's Divisions and Offices.

In addition, the FDIC did not have an effective enterprise architecture to support its IT decision-making and guide the execution of its strategic goals and objectives. We found that the FDIC's architecture was immature, and it did not guide the three IT initiatives we reviewed nor the FDIC's transition of IT services to the cloud.

Also, the FDIC had not established security architecture for its IT Governance Framework and IT Governance Processes, nor adequately defined the roles and responsibilities of information security officials. Notably, a third-party consultant assessed the FDIC's enterprise security architecture, noting it was "ad hoc" and was "inconsistently documented and implemented." The consultant further found that the FDIC's IT Governance Processes did not clearly document roles and responsibilities for IT security.

Moreover, the FDIC had not acquired adequate resources and expertise needed to improve the FDIC's IT Governance Framework and did not use complete cost information when evaluating cloud solutions. The FDIC's plans for significant and rapid transformation in the delivery of IT resources required individuals with expertise that the FDIC lacked in 2016 and improved financial information such as relevant intangible benefits to evaluate IT initiatives.

These challenges created uncertainty among FDIC Divisions and Offices regarding the implementation of the FDIC's IT strategic goals and objectives and the impact such efforts would have on their respective program areas. We also found that due to the limited IT governance applied to the cloud and laptop deployment initiatives that we reviewed, the former FDIC Chief Information Officer pursued overly aggressive implementation schedules and did not obtain broad business stakeholder involvement during the early stages of two of the three initiatives we reviewed. This resulted in unaddressed business needs and security risks, and it created inefficiencies, increased costs, and delayed the initiatives.

We made eight recommendations to address the IT Governance weaknesses we identified. These recommendations included the FDIC developing an implementation plan that supports the IT Strategic Plan; implementing an enterprise architecture as part of the IT Governance Framework; defining and documenting roles and responsibilities for information security; and identifying IT resources and expertise to execute the IT Strategic Plan.

Forward-Looking Supervision

The goals of the FDIC's Forward-Looking Supervision initiative are to identify and assess risk before it impacts a financial institution's financial condition and to ensure early risk mitigation. Our evaluation objective was to determine whether the Forward- Looking Supervision approach achieved its outcomes—the Division of Risk Management Supervision pursued supervisory action upon identifying risks and the financial institutions implemented corrective measures. Our review showed that examiners substantially achieved the intended outcomes of the Forward-Looking Supervision approach for our sampled institutions. Examiners applied Forward-Looking Supervision concepts during their financial institution examinations, rated institutions based on risk, and recommended corrective actions based on their risk assessments. Also, the financial institutions committed to implement the corrective actions.

We found that:

- The FDIC did not have a comprehensive policy guidance document on Forward-Looking Supervision and should clarify guidance associated with its purpose, goals, roles, and responsibilities;
- Examiners typically documented their overall conclusions regarding the financial institutions' concentration risk management practices; however, they did not always document certain Forward-Looking Supervision concepts in pre-examination planning documents and when reporting examination results;
- Examiners typically reported or elevated identified overall concentration risk management conclusions and concerns; however, a greater number of these concerns should have appeared in the report section that includes issues requiring the attention of the institution's board; and
- Examiners generally identified concentration risk management concerns on a timely basis; however, in certain instances, they identified concentration risk management concerns that had not been identified during the prior examination cycle.

We made four recommendations to the FDIC to: (1) issue a comprehensive policy guidance document defining Forward-Looking Supervision; (2) issue guidance to reinforce how and where examiners should be documenting concentrations and an institution's concentration risk management practices in the Report of Examination; (3) provide additional case studies on Forward-Looking Supervision to strengthen training for examiners; and (4) conduct recurring retrospective reviews to ensure examiners are documenting the concentration risk management analysis.

Claims Administration System Functionality

The FDIC's Claims Administration System (CAS) is a mission-critical system that FDIC personnel use to identify depositors' insured and uninsured funds in failing and failed financial institutions. CAS's capabilities affect the FDIC's ability to pay deposit insurance claims in a prompt and accurate manner. We evaluated the extent to which CAS has achieved the FDIC's

performance expectations for capacity, timeliness, and accuracy in making insurance determinations.

We found that CAS had substantially met the FDIC's expectations for capacity, timeliness, and accuracy in making insurance determinations for most insured institutions. Recognizing the difficulties in resolving a large institution over a closing weekend, the FDIC issued rules intended to mitigate potential shortfalls in CAS capability. The largest financial institutions (those with 2 million or more deposit accounts) are required to configure their information systems and data to enable the FDIC to make insurance determinations by April 2020. We recommended further simulation and testing for failing and failed large bank scenarios in order to facilitate resolution planning for potential large bank failures and decrease the risk of untimely insurance determinations.

The FDIC had not fully validated the maximum processing capacity of CAS. In the original justification for CAS in 2006, FDIC program officials initially expected that CAS could make insurance determinations for an institution of any size, up to 5 million deposit accounts. Because the FDIC recognized that it could not achieve this expectation due to the account complexities at larger institutions, the FDIC adjusted its expectations for institutions with up to 2 million deposit accounts.

CAS improved timeliness of insurance determinations compared to the FDIC's predecessor system. The FDIC's goal is to provide depositors at failed institutions with access to their insured funds within one or two business days of failure. Although the FDIC has never failed to meet this timeliness standard, CAS may not be able to meet the FDIC's goal for the largest institutions due to the volume and complexity of large bank deposit platforms. In such cases, it may be necessary for the FDIC to withhold a portion of the failed institution's deposits until an insurance determination can be made.

Regarding accuracy in making insurance determinations, CAS has reduced the risk of inaccurate insurance determinations as compared to the FDIC's predecessor system by decreasing the opportunity for human error. The FDIC believes that CAS capabilities and procedures provide reasonable assurance of the accuracy of insurance determinations.

We made three recommendations to improve CAS functionality through additional testing.

Processing of Consumer Complaints

The FDIC plays an important role in helping to protect consumers from unfair and unlawful banking practices that could result in consumer harm. In connection with that role, the FDIC receives, investigates, and answers consumer complaints and inquiries. We issued a report on the FDIC's Processing of Consumer Complaints, in which we assessed the FDIC's compliance with key requirements and determined how the FDIC used consumer complaint information and trends data in its operations.

FDIC personnel categorize complaints in one of two ways: "Fair Lending" complaints allege possible discrimination in lending under the Fair Housing Act or the Equal Credit Opportunity Act. Complaints that do not meet this definition are considered "Non-Fair Lending" cases. In 2017, the FDIC finalized 82 Fair Lending complaints and 3,907 Non-Fair Lending complaints.

We reviewed 60 complaint cases (22 Fair Lending and 38 Non-Fair Lending cases). We found that the FDIC substantially complied with the key requirements to acknowledge, investigate, and respond to the complaints that we sampled. However, we identified 32 case processing exceptions. The exceptions primarily involved instances when the FDIC did not include all required information in recommendation memorandums, which are prepared to document its review of Fair Lending cases and recommendations to conduct or waive on-site investigations at subject banks.

We also found that the FDIC did not process 45 percent of the Fair Lending cases that we sampled in accordance with its case processing timeframe of 120 days. The FDIC took from 126 to 506 days to process the Fair Lending cases that we sampled, with an average processing time of 284 days – nearly 9½ months. Five Fair Lending cases from our sample took more than 300 days for the FDIC to process, with one of these cases taking nearly 17 months. Similarly, the FDIC did not process 45 percent of its Fair Lending cases over the 3-year period from 2015 through 2017 in a timely manner.

As for Non-Fair Lending cases, we found that the FDIC did not process 11 percent of the cases that we sampled in accordance with its case processing timeframe of 60 days. Notably, however, the FDIC processed 95 percent of its Non-Fair Lending cases within 60 days from 2015 through 2017.

We made four recommendations to help ensure the FDIC includes all required information in recommendation memorandums and to help improve the FDIC's timeliness in processing Fair Lending cases.

FISMA Audit – 2018

In this audit, we evaluated the effectiveness of the FDIC's information security program and practices. The IG FISMA Reporting Metrics require IGs to assess the effectiveness of their agencies' information security programs and practices on a maturity model spectrum. We found that the FDIC's overall information security program was operating at a Maturity Level 3 (Consistently Implemented) on a scale of 1 to 5, which is an improvement from 2017, but not considered effective under the metrics.

We found that the FDIC established a number of information security program controls and practices that complied or were consistent with standards and guidelines, and took steps to strengthen controls following the 2017 FISMA report. However, ongoing security control weaknesses 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. In many cases, these security control weaknesses were identified by other OIG audits or through security control assessments completed by the FDIC. Although the FDIC was working to address these previously identified control weaknesses, the FDIC had not yet completed corrective actions at the time of the audit. Accordingly, the security control weaknesses continued to pose risk to the FDIC. The highest risk weaknesses included:

- **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. This limits the ability of FDIC Divisions and Offices to make effective risk management decisions, and prevents the FDIC from ensuring it is effectively prioritizing resources toward addressing risks with the most significant potential impact on achieving strategic objectives.

- **Enterprise Security Architecture.** Our 2017 FISMA audit noted that the FDIC had not established an enterprise security architecture, which is considered a fundamental component of an effective information security program and describes the structure and behavior of an organization's security processes, systems, personnel, and subunits and shows their alignment with the organization's mission and strategic plans. In July 2018, the FDIC provided the OIG with documentation describing its enterprise security architecture. The OIG is reviewing this documentation, along with other information related to the enterprise security architecture provided by the FDIC, to determine whether it is responsive to the recommendation in our FISMA audit report issued in 2017. The lack of 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.

- **Security Control Assessments.** In separate OIG audit work, we 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/or interviews of FDIC or contractor personnel. Without testing, assessors did not have a basis for concluding on the effectiveness of security controls. Inadequate FDIC oversight of security control assessments contributed to this weakness. Because the FDIC relies on the results of the assessments to support a number of important risk management activities, 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. Unpatched systems increase the risk of exposing the FDIC's network to a security incident.

- **Backup and Recovery.** Our 2017 FISMA report noted that the FDIC's IT restoration capabilities were limited and that the FDIC had not taken timely action to address known

limitations with respect to its ability to maintain or restore critical IT systems and applications during a disaster. In December 2017, the FDIC's Board of Directors authorized a multi-year Backup Data Center Migration Project to ensure that designated IT systems and applications supporting mission-essential functions can be recovered within targeted timeframes. While the FDIC established governance over this project, assurance that the FDIC can maintain and restore mission-essential functions during an emergency within applicable timeframes will be limited until the scheduled completion of the project in 2019.

We made four new recommendations to improve the effectiveness of the FDIC's information security program controls and practices.

Special Inquiry Report

In addition to the audit and evaluation reports listed above, the OIG issued a multi-disciplinary special inquiry report in April 2018. This special inquiry was conducted at the request of the Congress and involved significant effort by staff in our Office of General Counsel, Office of Investigations, and Immediate Office, with assistance and coordination from our Office of IT Audits and Cyber. A summary of this special inquiry follows.

The FDIC's Response, Reporting, and Interactions with Congress Concerning Information Security Incidents and Breaches

During late 2015 and early 2016, the FDIC experienced eight information security incidents as departing employees improperly took sensitive information shortly before leaving the FDIC. Seven of the eight incidents involved Personally Identifiable Information (PII), including Social Security Numbers, and thus constituted breaches. In the eighth incident, the departing employee took highly sensitive components of resolution plans submitted by certain large systemically important financial institutions without authorization.

In April and May 2016, the Committee on Science, Space, and Technology of the House of Representatives (SST Committee) examined the FDIC's handling of these incidents, its data security policies, and reporting of the "major incidents." As part of its investigation, the SST Committee requested pertinent documents from the FDIC about the incidents. The SST Committee held two hearings in May and July 2016 about the incidents at the FDIC and issued an interim report on the matter. During the hearings and in its interim report, as well in correspondence with the FDIC, the SST Committee expressed concerns about the FDIC's information security program, the accuracy of certain FDIC statements, and the completeness of the FDIC's document productions.

On June 28, 2016, the then-Chairman of the Senate Committee on Banking, Housing, and Urban Affairs requested that our Office examine issues at the FDIC related to data security, incident reporting, and policies, as well as the representations made by FDIC officials.

The FDIC OIG conducted a Special Inquiry in response to that request. We examined the circumstances surrounding the eight information security incidents. The FDIC initially estimated that the incidents involved sensitive information that included the PII of approximately 200,000 individual bank customers related to approximately 380 financial institutions, as well as the proprietary and sensitive data of financial institutions. Based on additional analysis, the FDIC later revised the number of affected individuals to 121,633.

Our work revealed certain systemic weaknesses that hindered the FDIC's ability to handle multiple information security incidents and breaches efficiently and effectively; contributed to untimely, inaccurate, and imprecise reporting of information to the Congress; and led to document productions that did not fully comply with Congressional document requests. We also identified shortcomings in the performance of certain individuals in key leadership positions as they handled the incidents and related activities.

Importantly, in its handling of the information security incidents, the FDIC did not fully consider the range of impacts on bank customers whose information had been compromised or consider customer notification as a separate decision from whether it would provide credit monitoring services. As a result, the FDIC delayed notifying consumers and thus precluded them from taking proactive steps to protect themselves. Also of note, when reporting incidents to the Congress, the FDIC used broad characterizations and referenced mitigating factors that were sometimes inaccurate and imprecise, and tended to diminish the potential risks. Despite several opportunities to clarify or correct the record regarding the nature of the incidents, the FDIC did not provide the Congress with accurate and complete information about the incidents. Finally, with regard to document production, the SST Committee had requested that the FDIC produce relevant documents and information. The FDIC did not initially respond to these requests in a complete manner and should have been clear in its communications with the Committee as to its approach and progress in complying with the document production requests. Later, the FDIC took steps to better identify and provide responsive records.

Throughout and subsequent to our Special Inquiry, the FDIC took steps to address prior recommendations pertaining to incident and breach response. In addition, we made 13 recommendations in this Special Inquiry report to address the systemic issues associated with the FDIC's incident response and reporting and interactions with the Congress. We also requested that the FDIC review the performance issues we identified and advise the OIG of actions taken to address them.

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 are therefore augmenting our resources to address such crimes.

During FY 2018, FDIC OIG investigations resulted in 67 indictments and informations; 62 convictions; 40 arrests; and fines, restitution ordered, and asset forfeitures exceeding $356 million. The following cases are illustrative of these OIG investigative accomplishments, achieved through collaborative efforts with Federal, state, and local law enforcement entities.

Former Global Head of HSBC's Foreign Exchange Cash Trading Sentenced to 24 Months' Imprisonment for Front-Running Scheme

On April 26, 2018, the former head of global foreign exchange cash trading at HSBC Bank plc, a subsidiary of HSBC Holdings plc, was sentenced to 24 months' imprisonment for committing wire fraud and wire fraud conspiracy, to be followed by 5 years of supervised release. He was also ordered to pay a $300,000 fine. The former bank executive was convicted by a federal jury in October 2017, following a 4-week trial, of one count of wire fraud conspiracy and eight counts of wire fraud.

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

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

Former Chief Executive Officer and Chief Loan Officer of Failed Sonoma Valley Bank, and Borrower's California Attorney Sentenced to Multi-Year Prison Terms for Bank Fraud and Other Crimes

On August 3, 2018, the former chief executive officer (CEO) and former chief loan officer (CLO) of Sonoma Valley Bank were sentenced for their December 2017 convictions for conspiracy, bank fraud, wire fraud, money laundering, falsifying bank records, lying to bank regulators, and other crimes. An attorney for a real estate developer involved in the scheme was also sentenced for his conviction on bank fraud, wire fraud, attempted obstruction of justice, and other offenses. The court sentenced the former CEO to 100 months in prison, the former CLO to 100 months in prison, and the attorney to 80 months in prison. The individuals were ordered to pay the government more than $19 million for their roles in the scheme.

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

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

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

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

On December 17, 2018, 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 pled 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, the former president defrauded the bank in several ways: (1) by issuing loans with insufficient collateral and falsifying financial statements for several high-dollar bank borrowers; (2) by originating nominee loans to circumvent the bank's legal lending limit; (3) by concealing the bank's true financial condition

from the Board of Directors; (4) by soliciting a fraudulent investment; and (5) by falsely representing the bank's true status to the FDIC.

Over a 4-year period, the former president 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. The former president misled the Board of Directors by falsely stating the borrowers were paying down their loans.

The former president also defrauded a partial owner and investor in the bank by convincing him to wire nearly $40 million. The former president 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, the former president 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 is due $40 million of the restitution amount, and the remaining $97 million is due to the FDIC, which lost money when it assumed the bank's liabilities as receiver in January 2014.

TOP CHALLENGES FACING THE FDIC

As required by statute, we identified the Top Management and Performance Challenges facing the FDIC. We conducted our research based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and other relevant literature, perspectives from government agencies and officials, and information from private sector entities in light of the current operating environment and circumstances.

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

Enhancing Oversight of Banks' Cybersecurity Risk

Cybersecurity continues to be a critical risk facing the financial sector. Cyber risks can affect the safety and soundness of institutions and lead to the failure of banks, thus causing losses to the FDIC's Deposit Insurance Fund. For example, a cybersecurity incident could disrupt services at a bank, resulting in the exploitation of personal information in fraudulent or other illicit schemes, and an incident could start a contagion that spreads through established

interconnected banking relationships. Despite increased spending on cybersecurity, banks are encountering difficulties in getting ahead of the increased frequency and sophistication of cyberattacks. The FDIC's IT examinations should ensure strong management practices within financial institutions and at their service providers.

Adapting to Financial Technology Innovation

FDIC policy makers and examiners must keep pace with the adoption of new financial technology to assess safety and soundness of institutions, and its impact on the stability of the banking system. The pace of change and breadth of innovation requires that the FDIC create agile and nimble regulatory processes, so that it can respond to and adjust policies, examination processes, supervisory strategies, preparedness and readiness, and resolution approaches as needed.

Strengthening FDIC Information Security Management

The FDIC maintains thousands of terabytes of sensitive data within its IT systems and has more than 180 IT systems that collect, store, or process the PII of FDIC employees; bank officials at FDIC-supervised institutions; and bank customers, depositors, and bank officials associated with failed banks. FDIC systems also hold sensitive supervisory data about the financial health of banks, bank resolution strategies, and resolution activities. The FDIC must continue to strengthen its implementation of governance and security controls around its IT systems to ensure that information is safeguarded properly.

Preparing for Crises

Central to the FDIC's mission is readiness to address crises in the banking system. The FDIC must be prepared for a broad range of crises that could impact the banking sector. These readiness activities should help to ensure the safety and soundness of institutions, as well as the stability and integrity of our nation's banking system.

Maturing Enterprise Risk Management

Enterprise Risk Management (ERM) is a critical part of an agency's governance, as it can inform prudent decision-making at an agency, including strategic planning, budget formulation, and capital investment. ERM program requirements include identifying risks that could affect the organization (Risk Profile and Inventory), establishing the amount of risk an organization is willing to accept (Risk Appetite), prioritizing strategies to address risks in the proper sequence, and responding to and mitigating the risks. The FDIC established an ERM program office in 2011, but has neither developed the underlying ERM program requirements nor realized the benefits of a mature ERM program.

Sharing Threat Information with Banks and Examiners

Federal Government agencies and private-sector entities share information about threats to U.S. critical infrastructure sectors, including the financial sector. Sharing actionable and

relevant threat information among Federal and private-sector participants protects the financial system by building threat awareness and allowing for informed decision-making. The FDIC must ensure that relevant threat information is shared with its supervised institutions and FDIC examiners as needed, in a timely manner, so that actions can be taken to address the threats. Threat information also provides FDIC examiners with context to evaluate banks' processes for risk identification and mitigation strategies.

Managing Human Capital

The FDIC relies on skilled personnel to fulfill its mission, and 68 percent of the FDIC's operating budget for 2019 ($1.8 billion) was for salaries and associated benefits for employees. Forty-two percent of FDIC employees are eligible to retire within 5 years, which may lead to knowledge and leadership gaps. To ensure mission readiness, the FDIC should find ways to manage this impending shortfall. In addition, the FDIC should seek to hire individuals with the advanced technical skills needed for IT examinations and supervision of large and complex banks.

Administering the Acquisitions Process

The FDIC relies heavily on contractors for support of its mission, especially for IT and administrative support services. The average annual expenditure by the FDIC for contractor services over the past 5 years has been approximately $587 million. The FDIC should maintain effective controls to ensure proper oversight and management of such contracts and should conduct regular reviews of contractors. In addition, the FDIC should also perform due diligence to mitigate security risks associated with supply chains for goods and services.

Improving Measurement of Regulatory Costs and Benefits

Before issuing a rule, the FDIC should ensure that the benefits accrued from a regulation justify the costs imposed. The FDIC should establish a sound mechanism to measure both costs and benefits at the time of promulgation, and it should continue to evaluate the costs and benefits of a regulation on a regular basis, even after it has been issued.

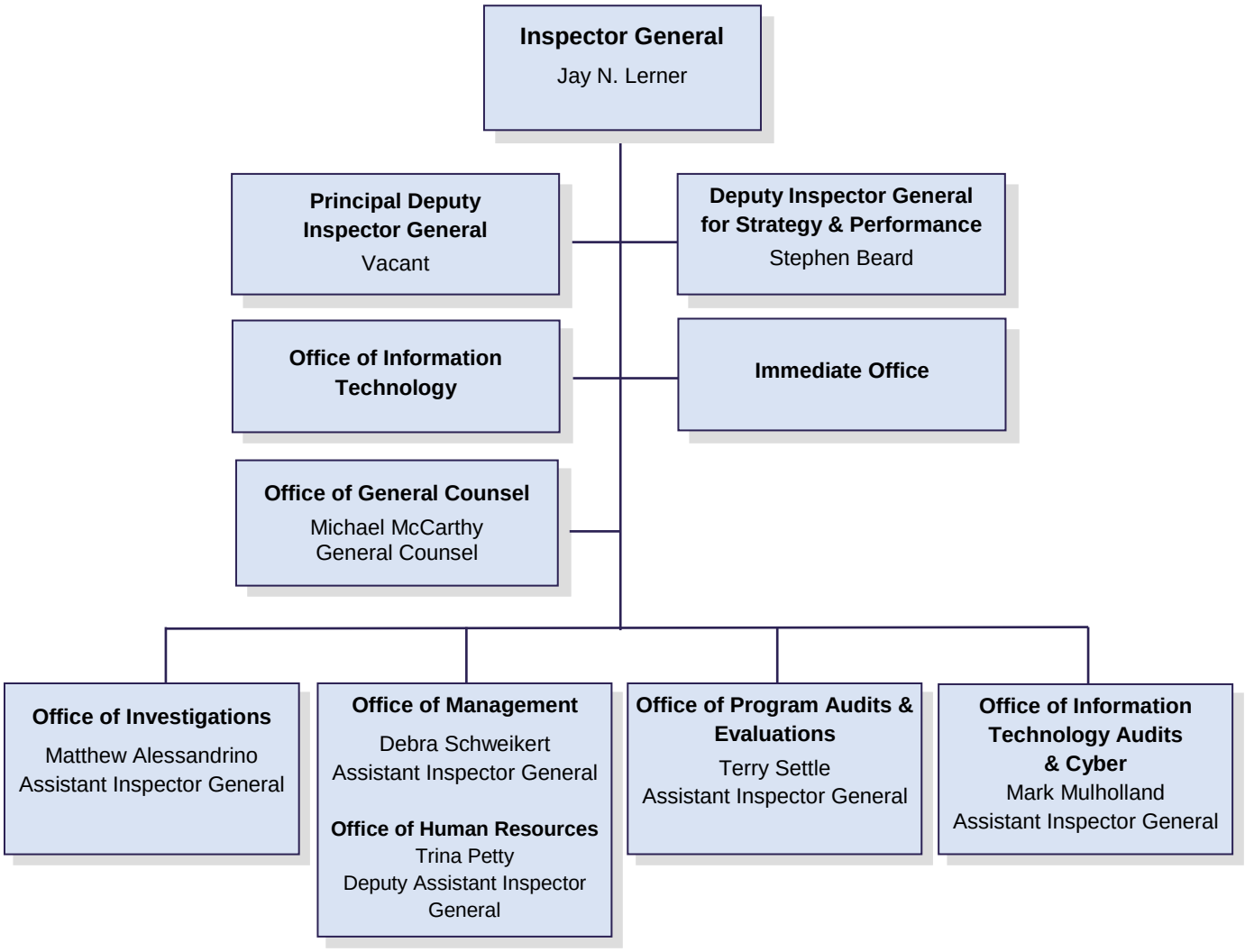
CONCLUSION

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 2020, 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 2020 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 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.

Appendix II OIG Accomplishments in FY 2018

In FY 2018, results of OIG audits, evaluations, and investigations were as follows:

Significant Outcomes (October 1, 2017 –September 30, 2018)	
Audit and Evaluation Reports Issued	8
Other Products Issued	3
Recommendations	62
Investigations Opened	60
Investigations Closed	74
Judicial Actions:	
Indictments/Informations	67
Convictions	62
Arrests	40
OIG Investigative Results:	
Fines	$153,562,460
Restitution Ordered	171,789,603
Asset Forfeitures	31,247,720
Total	**$356,599,783**

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 2018 Actual (000 omitted)**	**FY 2019 Budget (000 omitted)**	**FY 2020 Proposed (000 omitted)**
11.1 Full-Time Equivalent	$21,145	$24,049	$24,941
11.5 Other Personnel Compensation	837	947	850
11.9 Total Personnel Compensation	$21,982	$24,996	$25,791
12.0 Civilian Personnel Benefits	9,542	11,930	11,841
21.0 Travel and Transportation of Persons	958	1,307	975
22.0 Transportation of Things	0	14	14
24.0 Printing and Reproduction	0	0	0
25.0 Other Services *	2,527	1,827	2,754
26.0 Supplies and Materials	5	17	15
31.0 Equipment	2,921	2,891	1,592
Total Appropriation	**$37,935**	**$42,982**	**$42,982**

Personnel Summary	FY 2018 Actual	FY 2019 Budget	FY 2020 Proposed
Total Compensable Work Years:			
Staffing	128	144	144

* Other Services in FY 2020 includes $285,000 for training and $112,000 for support of the Council of the Inspectors General on Integrity and Efficiency.