Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2021

Federal Deposit Insurance Corporation
Office of Inspector General

Date: February 18, 2021

Memorandum To: Board of Directors

From: Jay N. Lerner
Inspector General

Subject Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

The Office of Inspector General (OIG) presents its annual assessment of the Top Management and Performance Challenges facing the Federal Deposit Insurance Corporation (FDIC). The purpose of this document is to summarize the most serious challenges facing the FDIC, and to briefly assess the Agency's progress to address them.

This Challenges document is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

We identified ten Top Challenges facing the FDIC. These Challenges include nine Challenges that we reported last year, with updates and revisions to identify changes resulting from the current pandemic, economic conditions, and other circumstances, as well as one additional Challenge on Supporting Diversity in Banking. The Top Challenges include:

1. Ensuring Readiness in a Pandemic Environment;
2. Mitigating Cybersecurity Risks in the Banking Sector;
3. Improving IT Security Within the FDIC;
4. Securing FDIC Personnel, Facilities, and Information;
5. Ensuring and Aligning Strong Governance at the FDIC;
6. Augmenting the FDIC's Sharing of Threat Information;
7. Supporting Diversity in Banking;
8. Managing Human Resources and Planning for the Future Workforce;
9. Overseeing Contracts and Managing Supply Chain Risk; and
10. Enhancing Rulemaking at the FDIC.

We believe that this researched and deliberative analysis will be beneficial and constructive for policy makers, including the FDIC and Congressional oversight bodies. We further hope that it is informative for the American people regarding the programs and operations at the FDIC and the Challenges it faces.

INTRODUCTION

The Office of Inspector General (OIG) presents this report, to identify the Top Management and Performance Challenges (TMPC) facing the Federal Deposit Insurance Corporation (FDIC). The purpose of this document is to summarize the most serious challenges facing the FDIC, and to briefly assess the Agency's progress to address them, pursuant to the Reports Consolidation Act of 2000 and the Office of Management and Budget Circular A-136 (revised August 27, 2020).

This TMPC document is based on the OIG's experience and observations from our oversight work, reports by other oversight bodies, review of academic and relevant literature, perspectives from Government agencies and officials, and information from private-sector entities.

We identified ten Challenges facing the FDIC. These Challenges include nine Challenges that we reported last year, with updates and revisions to identify changes resulting from the current pandemic, economic conditions, and other circumstances, as well as one additional Challenge on Supporting Diversity in Banking. We provide a brief introductory summary and a detailed discussion for each Challenge in the following document. The Challenges include:

1. Ensuring Readiness in a Pandemic Environment;
2. Mitigating Cybersecurity Risks in the Banking Sector;
3. Improving IT Security Within the FDIC;
4. Securing FDIC Personnel, Facilities, and Information;
5. Ensuring and Aligning Strong Governance at the FDIC;
6. Augmenting the FDIC's Sharing of Threat Information;
7. Supporting Diversity in Banking;
8. Managing Human Resources and Planning for the Future Workforce;
9. Overseeing Contracts and Managing Supply Chain Risk; and
10. Enhancing Rulemaking at the FDIC.

To compile this document, we received input and considered comments from the FDIC, and while exercising our independent judgment, we incorporated suggestions where appropriate and fair. In several instances, we discuss topic areas where the OIG had previously conducted work to evaluate and audit the FDIC's progress in these Challenge areas. We commend the FDIC for taking steps in some areas to address certain Challenges, and we note many of these actions in the attached document, particularly where the Agency has taken concrete and measurable steps that demonstrate a clear and direct relationship towards achieving positive results and a desired outcome. We also recognize that there may be other ongoing plans, inputs, intentions, or future activities that might still be under development at the time of this writing.

We believe that this researched and deliberative analysis will be beneficial and constructive for policy makers, including the FDIC and Congressional oversight bodies. We further hope that it is informative for the American people regarding the programs and operations at the FDIC and the Challenges it faces.

Challenge 1: Ensuring Readiness in a Pandemic Environment

Global economies are experiencing stress from the Covid-19 pandemic. In the United States, more than 30 million small businesses have been affected by current economic conditions, and claims for unemployment compensation have risen sharply. As a result, individuals and businesses may not be able to meet their debt obligations to financial institutions. Loan defaults may increase as pandemic-related economic pressures continue, and banks may struggle. The FDIC should continue to stand ready to fulfill its mission to maintain financial stability in the banking system, and to identify and mitigate risks through examinations. The FDIC should also prepare for bank failures in the event that losses overwhelm banks. Further, through its supervisory processes, the FDIC should review banks' adherence to Government-guaranteed loan program requirements (like the Paycheck Protection Program) and identify fraud, operational, legal, and reputational risks that may affect the safety and soundness of a financial institution.

The Financial Stability Oversight Council (FSOC)[1] stated that the pandemic has been "an extraordinary shock to the global financial system."[2] The World Bank projects that protracted viral outbreaks may disrupt economic activity, thus causing businesses to confront difficulties in servicing debt and increasing the cost of borrowing.[3] As a result, bankruptcies and defaults may increase, and banks may struggle.[4]

In the United States, pandemic-related unemployment and reduced business activity have already affected the ability of households and businesses to meet their financial obligations. FSOC noted that nearly $2 trillion in corporate debt has been downgraded, and default rates on loans and corporate bonds have increased considerably.[5] Certain loan categories such as commercial real estate loans reportedly had delinquency rates

[1] FSOC was created by the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) and is responsible for identifying threats to the financial stability of the country, promoting market discipline, and responding to emerging risks to the stability of the nation's financial system. Pub. L. No. 111-203, §111, 124 Stat 1376, 1392-3 (2010). FSOC consists of 10 voting members and 5 non-voting members. FSOC voting members include: The Secretary of the Treasury, Chairman of the Board of Governors of the Federal Reserve System, Comptroller of the Currency, Director of the Bureau of Consumer Financial Protection, Chairman of the Securities and Exchange Commission, Chairman of the Federal Deposit Insurance Corporation, Chairman of the Commodity Futures Trading Commission, Director of the Federal Housing Finance Agency, Chairman of the National Credit Union Administration, and an independent member having insurance expertise who is appointed by the President and confirmed by the Senate for a 6-year term. The non-voting members include the Director of the Office of Financial Research, the Director of the Federal Insurance Office, a state banking supervisor, state insurance commissioner, and state securities commissioner.

[2] FSOC, *Annual Report 2020*, (December 3, 2020).

[3] The World Bank, *The Global Economic Outlook During the COVID-19 Pandemic: A Changed World*, (June 8, 2020).

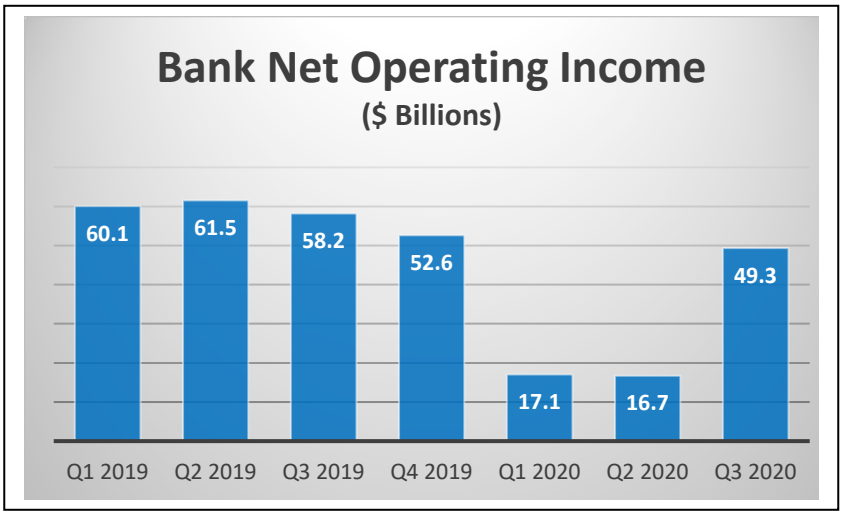
[4] The World Bank, *The Global Economic Outlook During the COVID-19 Pandemic: A Changed World*, (June 8, 2020).

[5] FSOC, *Annual Report 2020*, (December 3, 2020).

of 8.3 percent (representing $45 billion in loans) as of October 2020;[6] about 40 percent of community banks' loan portfolios are comprised of commercial real estate loans.[7] As of December 2020, the data analytics firm Black Knight reported that 5.2 percent of home mortgages in the United States (2.75 million homeowners) were in forbearance programs that allowed them to delay monthly mortgage payments.[8]

As shown in Figure 1, net operating income at banks declined 67 percent from the fourth quarter of 2019 to the first quarter of 2020. Bank net operating income declined further to $16.7 billion in the second quarter of 2020. Although it improved to $49.3 billion in the third quarter of 2020, it remained $8.9 billion less than the $58.2 billion during the same period in 2019.

Figure 1: Bank Net Operating Income 2019-2020 by Quarter



Source: FDIC Quarterly Banking Profile, Third Quarter 2020 Chart 1.

The duration and severity of the pandemic's impact on the economy is uncertain at the present time. A study of small business conducted by researchers at Yale, Princeton, and Oxford Universities found that loan defaults and delinquencies may continue to rise with banks suffering additional losses.[9] In June 2020, the Congressional Research Service noted that 87 banks were in danger of becoming seriously distressed,[10] and in November 2020, it was reported that 50 banks were considered to be troubled, meaning that they may not have sufficient capital to cover their losses.[11] As of the third quarter of 2020, the FDIC reported 56 banks were on the FDIC's problem bank list, an increase from 52 banks in the second quarter of 2020.[12]

The mission of the FDIC is to maintain the stability of the nation's financial system by examining and supervising financial institutions, insuring customer deposits, and managing the Deposit Insurance Fund. The FDIC examines the safety and soundness

---

[6] The Washington Post, *Mounting Commercial Real Estate Losses Threaten Banks, Recovery*, (November 11, 2020).
[7] FSOC, *Annual Report 2020*, (December 3, 2020).
[8] Black Knight, *New Forbearance Starts Increase as Overall Volumes See First Monthly Rise Since Early June*, (December 11, 2020).
[9] Yale News, *Survey Shows Pandemic's Severe Impact on U.S. Small Businesses*, (May1,2020), noting a study projecting that 25 percent of small business owners do not expect to recover from the pandemic and 31 percent believe they have a 50-percent chance of going bankrupt.
[10] Congressional Research Service, *COVID-19 and the Banking Industry: Risks and Policy Responses*, (June 18, 2020).
[11] USA Today, *Two Small Banks Failed in October, They Won't Be The Last If COVID Leaves Some Businesses Struggling To Pay Loans*, (November 20, 2020).
[12] FDIC Quarterly Banking Profile, Third Quarter 2020, Chart 8. Problem banks "refer to institutions that exhibit deficiencies in practices or performance so severe that failure is either a distinct possibility (4 rating) or likely (5 rating) unless the deficiencies are corrected." FDIC, *Crisis and Response: An FDIC History, 2008-2013*.

of its supervised financial institutions by assessing banks' practices to manage and address risks at the institutions. The FDIC oversees banks' risk management in a variety of risk areas, including, for example, credit, liquidity, interest rate, operational, reputational, and compliance risk.

To accomplish its mission, the FDIC examines most of the financial institutions in the country (approximately 3,500 of the 5,000 banks). Also, the FDIC manages the resolution and receivership of failed banks, and its Deposit Insurance Fund (more than $116 billion as of the third quarter of 2020) insures approximately $8.9 trillion in customer deposit accounts held at domestic banks. The FDIC anticipates and is preparing for increased hiring to ensure readiness for any potential increase in supervisory workload, bank failure activity, and administrative support. The FDIC's Operating Budget for 2021 rose by $261 million (12.9 percent), largely due to "contingency reserves to address a potential increase during 2021 in supervision or resolution workload resulting from the ongoing pandemic."[13]

Identifying and Mitigating Risks to the Safety and Soundness of Institutions

FDIC bank examinations "play a key role in the supervisory process by helping the FDIC identify the cause and severity of problems at individual banks and emerging risks in the financial-services industry."[14] According to the Federal Reserve Bank of New York, "[t]he overarching objective of supervision is to identify and remediate conditions that could threaten banks' immediate health or long-term viability."[15] The FDIC uses models and examinations to identify banks' risks and assess whether banks mitigate these risks before they affect the safety and soundness, and condition of financial institutions.

Modeling Effects on Financial Institutions. The FDIC should continue to monitor the health of the banking sector in order to identify and respond to emerging economic strain and growing systemic risks. Timely risk identification allows the FDIC to adjust supervisory strategies and prepare for possible bank failures.

To do so, the FDIC relies upon data from a number of sources, including banks' quarterly Consolidated Reports of Condition and Income (Call Reports), which include banks' balance sheets, income statements, and supporting schedules.[16] FDIC economists and analysts face challenges in making real-time assessments of banks' current health and projecting future economic impact, because there is a lag time between the bank's actual financial condition and when the Call Report is submitted to the FDIC. This delay is nearly 4 months. The FDIC Chairman compared this information gap to a doctor trying to assess a patient's health today, but getting lab results 4 months later.[17] As a result, the FDIC is challenged to assess the current financial condition of an institution, in order to identify "key indicators of economic strain

[13] *Proposed 2021 FDIC Operating Budget*, (December 1, 2020).
[14] FDIC Division of Risk Management Supervision, *Risk Management Manual of Examination Policies*.
[15] Federal Reserve Bank of New York Staff Report, *The Impact of Supervision on Bank Performance*, (May 2019).
[16] 12 C.F.R. §304.3(a). The FDIC also uses a number of tools to monitor banks' liquidity and interest rate risk.
[17] FDIC Chairman Jelena McWilliams op-ed published in the American Banker's "BankThink" blog, *FDIC Chief on Why Call Reports Are Getting a Makeover* (July 1, 2020).

in the economy, growing stress across the financial system, and emerging risk at individual institutions."[18]

In addition, Call Reports do not capture certain information necessary for the FDIC to assess banking risk to the safety and soundness of institutions. For example, Call Report data do not identify high concentration exposures to certain sectors of the economy. A bank's concentration in particular types of loans may indicate undue risk at the institution. The FDIC should also consider using additional economic and financial information from other Government agencies and the private sector in order to enhance its current modeling and measurement of banking conditions and to evaluate the safety and soundness of institutions. We have work planned to assess FDIC modeling and its analysis of relevant information.

In June 2020, the FDIC announced a competition to improve financial reporting from banks. The FDIC asked certain technology companies for ideas and suggestions regarding new approaches to financial reporting, particularly for community banks.[19] As the FDIC considers this information received, it should also look for ways to improve its modeling capabilities and to anticipate weaknesses in the safety and soundness at banks, potential failures or closures, and risk factors facing the institutions.

Conducting Examinations Remotely. The Federal Deposit Insurance Act requires on-site, full-scope examinations of every FDIC-insured financial institution at least once during each 12-month period (with certain limited exceptions).[20] In March 2020, the FDIC mandated telework for its staff and continued all examination activities off site. Remote examinations may limit examiners' ability to conduct transaction testing. For example, examiners may not be able to observe processes in order to ensure that bank staff execute activities consistent with the bank's written policies and procedures.[21]

In May 2020, the FDIC modified its processes to allow for off-site examination activities to qualify as full-scope examinations under certain circumstances.[22] As part of these modifications, the FDIC used technology to observe certain bank processes such as examiners' assessments of banks' physical security through remote facility tours and remote access. If examiners could not complete examination modules or assign a rating without an on-site presence, then the examination would be "held in abeyance." A total of 39 FDIC examinations (2.9 percent of all FDIC examination starts) were held in abeyance for short periods of time during 2020. None of these examinations were held in abeyance at the end of the year.

Current social distancing guidelines also place an unexpected reliance on information technology (IT) systems to conduct FDIC examinations. A significant portion of bank examinations involve the exchange of documents and sensitive data, including bank information and customer data. Although the FDIC frequently exchanges data with banks through file exchange systems, the FDIC should continue to ensure that its

---

[18] FDIC Chairman Jelena McWilliams op-ed published in the American Banker's "BankThink" blog, *FDIC Chief on Why Call Reports Are Getting a Makeover* (July 1, 2020).
[19] FDIC Press Release, *FDIC Launches Competition to Modernize Bank Financial Reporting*, (June 30, 2020).
[20] 12 C.F.R. § 337.12.
[21] Bloomberg Law, *Bank Exams May Lose Punch as Coronavirus Restrictions Linger,* (March 18, 2020).
[22] FDIC Memorandum, *Temporary Examination Processes,* (May 5, 2020).

systems can accommodate the increased data flow and volume, as well as ensure the IT security and privacy associated with such transfers. Smaller banks may not have digital records[23] and staff capacity to transition from traditional mail-in records to secure online portals.[24] Such dependence on remote off-site examinations places a greater emphasis and focus on information security protocols and the reliability of the FDIC's information systems.

Ensuring the FDIC's Readiness for Crises

The FDIC should be prepared for a broad range of crises that could impact the banking system, and readiness plans and activities are an important part of this preparation. Readiness planning provides the ability to respond timely and effectively to crisis events. In our recent report, *The FDIC's Readiness for Crises* (April 2020), we found that the FDIC should fully establish seven elements of crisis readiness to be prepared for any type of crisis that may impact the banking system, including a pandemic. Specifically, we determined that the FDIC could improve the following elements of its crisis readiness framework:

- **Policy and Procedures:** The FDIC did not have a documented Agency policy that defined readiness authorities, roles, and responsibilities, including those of a committee responsible for overseeing readiness activities.
- **Plans:** The FDIC should develop an Agency-wide all-hazards readiness plan that identifies the critical common functions and tasks necessary regardless of the crisis scenario, as well as Agency-wide hazard-specific plans, as needed, to integrate divisional plans containing requirements unique to certain types of crises.
- **Training:** The FDIC did not train personnel to understand the content of crisis readiness plans, including their task-related responsibilities in executing the plans. Further, the FDIC did not incorporate a requirement within eight readiness plans to train responsible personnel to understand the plan, and how to carry out the objectives and tasks specific to the plan.
- **Exercises:** The FDIC should document the important results of all readiness plan exercises and consistently incorporate within the plans a requirement for regular exercises.
- **Lessons Learned:** The FDIC did not have a documented monitoring process that prioritized and tracked recommendations to improve readiness.
- **Maintenance:** The FDIC should consistently review and update readiness plans, incorporate maintenance requirements in the plans, and establish a central repository of plans to facilitate periodic maintenance.
- **Assessment and Reporting:** The FDIC should regularly assess and report on Agency-wide progress on crisis readiness plans and activities to key decision makers, such as the FDIC Chairman and senior management.

We made 11 recommendations to the FDIC to improve crisis readiness planning. The FDIC concurred or partially concurred with all of the recommendations. According to

[23] American Banker, *Will coronavirus hasten arrival of fully remote bank exams?,* (May 1, 2020).
[24] FDIC Financial Institution Letter, *Temporary Alternative Procedures for Sending Supervision-Related Mail and Email to the FDIC* (FIL-27-2020) (March 26, 2020).

FDIC officials, the Agency is in the process of addressing the recommendations, and it has hired outside consultants to assist in this effort. The FDIC also indicated that it has revised its resolution procedures to address the health and safety of on-site personnel and current pandemic conditions.

Resolving Financial Institutions

When a financial institution fails, the FDIC is responsible for facilitating the transfer of the institution's insured deposits to an assuming institution or paying insured depositors directly. Carrying out this responsibility during the pandemic necessitates health and safety considerations, because some resolution activities require FDIC personnel to be present at the failed bank offices and branches.

During 2020, the FDIC resolved several banks using a modified resolution process that the FDIC stated addressed pandemic health and safety requirements. The FDIC should be prepared to scale these new resolution processes for large bank or multi-bank failures and re-evaluate on-site procedures in light of evolving pandemic health and safety requirements.

In addition, in 2010, the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act) provided the FDIC with additional resolution authority for large complex financial companies known as systemically important financial institutions (SIFI). These provisions allow for liquidation of a bank where its bankruptcy would have serious adverse consequences on the financial stability of the United States, and where there is no private-sector alternative to prevent default.

Under Dodd-Frank Act authority, the FDIC is appointed as a receiver to carry out the liquidation of SIFIs. As such, the FDIC may take steps to transfer or sell assets, create bridge financial organizations to assume assets or liabilities, and approve claims against the failed bank. To help fund this liquidation process, the Dodd-Frank Act includes a separate Orderly Liquidation Fund created by the Department of the Treasury. In the event of an orderly liquidation of a SIFI, the FDIC should ensure that the Department of the Treasury has the required funds available for FDIC borrowings. Although the FDIC and other Federal agencies have conducted simulations of Dodd-Frank Act processes, the Federal Government has never invoked these Orderly Liquidation authorities.

Assessing Banks' Risk Regarding Government-Backed Loans

In response to the current pandemic, in March 2020, the Federal Government established the Paycheck Protection Program (PPP), among other programs, under the Coronavirus Aid, Relief, and Economic Security (CARES) Act.[25] The CARES Act was intended to provide economic relief to those in need during the pandemic.[26]

[25] The PPP was established by the Coronavirus Aid, Relief, and Economic Security Act (CARES Act). PL 116-136, 134 Stat 281 (2020). The program is implemented by the Small Business Administration with support from the Department of the Treasury. The program provides small businesses with funds to pay up to 8 weeks of payroll costs, including benefits. Funds can also be used to pay interest on mortgages, rent, and utilities.

[26] SBA, *Business Loan Program Temporary Changes: Paycheck Protection Act*, 85 Fed. Reg. 73 (April 15, 2020).

To date, the PPP has allocated more than $800 billion for banks to provide Government-guaranteed loans to eligible small businesses. As of the end of Fiscal Year 2020, 5,460 banks had processed 5.2 million PPP loans.[27] FDIC-supervised community banks originated over half of these PPP loans totaling more than $230 billion, and balance sheets at some banks grew by more than 25 percent as a result of these loans.[28]

Guaranteed-loan programs could lead to safety and soundness risk at financial institutions. For example, banks may suffer legal and reputational risk if banks do not follow Government-backed loan issuance requirements or where loan proceeds are used to facilitate financial fraud or other wrongdoing. According to the Small Business Administration Office of Inspector General (SBA OIG), approximately $3.6 billion in PPP loans were provided to potentially ineligible recipients,[29] and as of December 2020, the Department of Justice had initiated more than 65 criminal fraud charges related to the PPP involving over $250 million in PPP loans.

We recognize that the initial PPP was constructed in an effort to meet the urgent needs of small businesses and their employees. The banks nevertheless retain responsibilities to maintain strong compliance programs and internal controls over their loan portfolios. These responsibilities are not intended to deter, delay, or hamper bank loans to those in need, limit loans to eligible borrowers, nor hinder the implementation of the Government program. Through its supervisory processes, the FDIC should continue to examine banks' adherence to Government-guaranteed loan program requirements, and assess the risk of these loan portfolios. The FDIC provided guidance to examination staff on examiner considerations for the PPP.[30]

The impact of the pandemic on the banking system remains uncertain. Economic pressures may require that banks absorb additional losses that could result in bank weaknesses or failures. The FDIC should continue to identify and address emerging risks—including those related to Government-guaranteed loans—and be prepared to address bank failures.

---

[27] SBA OIG, *Top Management and Performance Challenges Facing the Small Business Administration in Fiscal Year 2021*, (October 16, 2020).
[28] American Banker, *Regulators Grant Relief to Banks Pushed Past Key Asset Limits by PPP*, (November 20, 2020).
[29] SBA OIG, *Top Management and Performance Challenges Facing the Small Business Administration in Fiscal Year 2021*, (October 16, 2020); SBA OIG, *Paycheck Protection Program Loan Recipients on the Department of Treasury's Do Not Pay List*, (January 11, 2021).
[30] FDIC, Risk Management Supervision Memorandum, Examination Considerations Related to the Paycheck Protection Program, (June 22, 2020).

Challenge 2: Mitigating Cybersecurity Risks in the Banking Sector

In recent months, cyberattacks against banks have increased with growing frequency and severity. The Federal Reserve Bank of New York estimated that financial services firms face up to 300 times the cybersecurity risk than do other businesses. This risk may intensify with remote work by employees at financial firms and enhanced customer convenience and access during the pandemic. The FDIC should ensure that it has IT examination processes and staff with the requisite skills to identify and mitigate cybersecurity risks at banks, including those associated with third-party service providers. Further, FDIC examination and resolution policies should keep pace with emerging cybersecurity issues facing the banking sector.

In April 2020, the Financial Stability Board (FSB) noted that cybersecurity incidents could undermine the integrity of global financial markets, causing losses to investors and the public.[31] In January 2020, the FDIC and Office of the Comptroller of the Currency (OCC) released a joint statement warning banks that "disruptive and destructive attacks against financial institutions have increased in frequency and severity in recent years."[32] A study by the Federal Reserve Bank of New York noted that financial services firms face up to "300 times more cyberattacks per year than other firms."[33]

The OCC expects cyber threats to banks, customers, and third parties to increase for the foreseeable future,[34] including destructive malware,[35] ransomware,[36] and phishing.[37] The Federal Bureau of Investigation's (FBI) Internet Crime Complaint Center[38] reported that in 2019, it received 2,047 complaints of ransomware.[39] According to a report by the cybersecurity company Arctic Wolf, in the first 3 months of the pandemic (between March and June 2020), ransomware and phishing attacks at banks increased by 520 percent.[40]

In October 2020, the Financial Crimes Enforcement Network (FinCEN) and the Office of Foreign Asset Control issued alerts to financial institutions about indicators of

[31] Financial Stability Board, *Effective Practices for Cyber Incident Response and Recovery: Consultative Document*, (April 20, 2020).
[32] FDIC and OCC, *Joint Statement on Heightened Cybersecurity Risk*, (January 16, 2020).
[33] Federal Reserve Bank of New York Staff Report, *Cyber Risk and the U.S. Financial System: A Pre-Mortem Analysis*, (January 2020).
[34] OCC, *Semiannual Risk Perspective*, (Spring 2020).
[35] Malware includes viruses, malicious code, spyware, and other computer programs that are covertly placed on a computer or systems "to compromise the confidentiality, integrity, or availability of data, applications, or operating systems." See National Institute of Standards and Technology, Glossary of Terms.
[36] Ransomware refers to computer software covertly placed on a computer or system that denies access to a user's data by encrypting the data. The data are released when the user pays a ransom to the hacker to receive the key to unlock the encryption. See National Institute of Standards and Technology, Glossary of Terms.
[37] Phishing is a technique to acquire access to a system through fraudulent solicitation in an email or website. See National Institute of Standards and Technology, Glossary of Terms.
[38] The FBI's IC3 provides the public with a mechanism for reporting information concerning suspected Internet-facilitated criminal activity.
[39] FBI, *Internet Crime Report 2019*.
[40] Artic Wolf, *2020 Security Operations Annual Report*.

ransomware and associated money laundering activities and sanction risks for facilitating ransomware payments.[41] Further, in April 2020, the Department of Homeland Security (DHS) released a joint alert with the United Kingdom's National Cyber Security Centre, to warn individuals and organizations about exploitation involving phishing schemes designed to look like they originated from a bank.[42] Also, in the same month, the FBI warned the public of an anticipated increase in phishing schemes known as Business Email Compromise schemes.[43]

According to the OCC's *Semiannual Risk Perspective* (Spring 2020),[44] banks have increased the integration of new technologies and technical capacity into their operations in order to accommodate customers' need for physical distancing and remote transactions. For example, banks are enabling new online and mobile banking services for customers' convenience, and allowing telework capabilities for bank personnel.[45] In April 2020, according to Fidelity National Information Services, mobile banking traffic increased 85 percent.[46]

The OCC warned that cyberattacks on financial institutions often focus on the use of virtual private networks, teleconferencing services, and remote telecommunication technologies.[47] Remote access systems that are not properly secured can "serve as gateways from the internet into internal networks, often offering immediate, highly privileged access to attackers."[48]

In addition, financial institutions, especially community banks, are relying on third-party service providers (TSP) to deliver such technology services.[49] These new technologies and third-party relationships increase the number of ways that cyberattacks can occur and their many entry points. For example, the OCC noted that cybercriminals circumvent bank cyber controls by targeting third-party providers.[50]

Financial institutions are increasingly reliant on TSPs to provide specialized products and critical IT services to supplement or increase their capabilities.[51] For example, the

---

[41] U.S. Department of the Treasury, Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, (October 1, 2020); U.S. Department of the Treasury, Office of Foreign Asset Control, *Advisory on Potential Sanctions for Facilitating Ransomware Payments*, (October 1, 2020). FinCEN is a component of the Department of the Treasury that collects and analyzes financial transaction information provided by the financial industry to combat money laundering, terrorist financing, and other financial crimes. FinCEN issues public and non-public advisories to financial institutions detailing activities and factors related to money laundering and terrorist financing threats and vulnerabilities so that financial institutions can use that information to enhance their anti-money laundering programs.

[42] DHS, CISA, and United Kingdom's National Cyber Security Centre Alert, *COVID-19 Exploited by Malicious Cyber Actors*, (April 8, 2020).

[43] Forbes, *Business Email Compromise Is Extremely Costly and Increasingly Preventable*, (April 15, 2020).

[44] OCC, *Semiannual Risk Perspective*, (Spring 2020).

[45] OCC, *Semiannual Risk Perspective*, (Spring 2020).

[46] CNBC, *Coronavirus Crisis Mobile Banking Surge Is a Shift That's Likely to Stick*, (May 27, 2020).

[47] OCC, *Semiannual Risk Perspective*, (Spring 2020).

[48] NextGov, *NSA Warns China IS Targeting Flaws in U.S. National Security Systems*, (October 20, 2020).

[49] Michelle W. Bowman, Governor, Board of Governors of the Federal Reserve System, *"Empowering Community Banks,"* delivered at the Conference for Community Bankers sponsored by The American Bankers Association; Orlando, Florida, (February 10, 2020).

[50] OCC, *Semiannual Risk Report*, (Fall 2019).

[51] OCC, *Semiannual Risk Perspective*, (Fall 2019); FSOC, *Annual Report 2020*.

OCC's *Semiannual Risk Perspective* (Spring 2020) noted that banks are further leveraging TSPs in this pandemic environment, in order to support remote work capabilities, technological capacity, and solutions to maintain operations virtually.[52] In addition, significant consolidation among TSPs drives large numbers of banks—especially community banks supervised by the FDIC—to rely on a few large service providers for core systems and operations support.[53] Therefore, a cybersecurity incident at one TSP has the potential to affect multiple financial institutions that could cause "widespread disruption in access to financial data and could impair the flow of financial transactions."[54]

Ensuring that Examinations Detect and Mitigate Cybersecurity Risk

According to the *Interagency Guidelines Establishing Information Security Standards* issued by Federal financial regulators,[55] a financial institution is responsible for the cybersecurity of its IT systems. Similarly, responsibility for compliance with consumer protection laws and regulations lies with the financial institution, regardless of whether the institution or a TSP controls the information.[56]

The FDIC assesses whether bank management has appropriate controls in place to mitigate cybersecurity risks through its IT risk examinations. Since 2016, the FDIC has used the Information Technology Risk Examination (InTREx) work program to conduct bank IT examinations and assess financial institutions' management of TSPs. The FDIC developed InTREx to enhance its IT supervision by utilizing a risk-focused examination approach. Examiners determine the scope of an IT examination consistent with a bank's IT complexity and risk. For example, the scope of an IT examination may increase due to, among other things, the introduction of new technology or the addition of a TSP. The FDIC should ensure that its assessments accurately capture banks' IT complexity and that it has the processes, resources, and staff with appropriate skills to complete thorough examinations in a timely manner. We have work planned to assess the InTREx program.

Addressing Risks Posed by Third-Party Service Providers

The FDIC requires financial institutions to manage the risks associated with using TSPs. Bank management should demonstrate that appropriate controls are in place to manage system interconnections, interfaces, and access of TSPs and their sub-contractors.[57] Yet, many community banks often lack the resources to exercise appropriate due diligence in their selection of TSPs and maintain adequate oversight of TSPs.[58] A Governor of the Federal Reserve Board recognized this burden on community banks,

---

[52] OCC, *Semiannual Risk Perspective*, (Spring 2020).
[53] OCC, *Semiannual Risk Perspective*, (Spring 2018).
[54] FSOC, *Annual Report 2020*.
[55] These Interagency Guidelines can be found in the FDIC Rules and Regulations, Part 364, Appendix B.
[56] 12 C.F.R. Part 364, Appendix B. The FDIC, OCC, and Board of Governors of the Federal Reserve issued the Interagency Guidelines Establishing Information Security Standards. Financial Institution Letter 44-2008, Guidance for Managing Third-Party Risk (June 6, 2008).
[57] OCC, *Semiannual Risk Perspective*, (Spring 2018).
[58] Michelle W. Bowman, Governor, Board of Governors of the Federal Reserve System, *"Empowering Community Banks,"* delivered at the Conference for Community Bankers sponsored by The American Bankers Association; Orlando, Florida, (February 10, 2020).

stating that "due diligence for new third-party relationships, even those that are not start-ups, can require a community bank to collect and analyze a significant amount of complex information [and] annual monitoring that is required adds an additional significant and ongoing burden." [59]

The FDIC assesses the risk associated with services provided by TSPs to banks through an examiner's assessment of the financial institution's management of TSP risk and, in certain cases, through direct examination of the services provided.[60] The FDIC Chairman has observed that "the FDIC had 'limited ability' to examine third-party service providers."[61] FSOC noted in its 2020 Annual Report, that the authority to supervise TSPs varies among financial regulators. Bank regulators, for example, write rules, publish guidance, and enforce compliance respecting banks' interactions with TSPs, but they do not regulate the TSPs.[62] FSOC recommended that agencies be authorized to oversee TSPs with examination and enforcement powers. For the time being, the FDIC is relying on its examination program to evaluate TSP security controls.

The FDIC plays an important role in supervising, examining, and addressing cybersecurity risks at financial institutions. These risks have the potential to threaten the safety and soundness of institutions as well as the stability of the financial system. The FDIC should continue to ensure it has the proper procedures and personnel with the appropriate skills, experience, and background in order to conduct effective IT examinations and assess management of cybersecurity risks, including risks associated with TSPs.

Challenge 3: Improving IT Security Within the FDIC

Federal agencies face a growing risk of cybersecurity incidents. In Fiscal Year 2019, Federal agencies reported 28,581 cybersecurity incidents. The rapid transition to remote work in response to pandemic protocols amplifies the Government's reliance on IT systems and accelerates implementation of technologies. Similarly, over the past year, the FDIC moved to a fully remote workforce and began implementing a 5-year plan to modernize its IT systems. The FDIC must have robust controls to secure its systems and ensure the protection of its information and data.

[59] Michelle W. Bowman, Governor, Board of Governors of the Federal Reserve System, *"Empowering Community Banks,"* delivered at the Conference for Community Bankers sponsored by The American Bankers Association; Orlando, Florida, (February 10, 2020).
[60] Under the Bank Service Company Act, certain services provided to banks may be subject to interagency examination by Federal regulators, including the FDIC. 12 U.S.C.§ 1867 (2011); *see* Federal Regulatory Agencies' Administrative Guidelines, *Implementation of Interagency Programs for the Supervision of Technology Service Providers*, (October 2012).
[61] CNN, *Banks could get fined for cyber breaches, top regulator says*, (August 1, 2019).
[62] Congressional Research Service, *Fintech: Overview of Financial Regulators and Recent Policy Approaches*, (April 28, 2020).

In its Annual Report to Congress, the Office of Management and Budget (OMB) reported that 28,581 cybersecurity incidents occurred at Federal agencies in Fiscal Year 2019. The Government Accountability Office (GAO) has identified cybersecurity as a High Risk across the Federal Government each year since 1997.[63] According to the GAO, "Federal agencies face a growing number of cyber threats to their systems and data."[64] These dangers include insider threats from both bad actors and unwitting employees, escalating and emerging threats from around the globe, and the emergence of new and destructive attacks. The pandemic has exacerbated cybersecurity threats targeting Federal agencies, including financial regulators, whose workforces transitioned to remote work.[65]

Recent events emphasize the vulnerability of Federal networks. In December 2020, it was reported that Federal Government agency networks were compromised by a software update from the IT management services company SolarWinds,[66] and that nation-state actors had inserted malicious code into the software update, which gave hackers access to Government systems.[67] The Cybersecurity and Infrastructure Security Agency (CISA) issued Emergency Directive 21-01, *Mitigate SolarWinds Orion Code Compromise*, to Federal agencies "to review their networks for indicators of compromise and disconnect or power down their SolarWinds Orion products immediately."[68] CISA reported that the threat from the SolarWinds compromise poses a great risk to the Federal Government.[69]

The FDIC uses a SolarWinds product. Following the issuance of the Emergency Directive, FDIC officials represented that they had disconnected the FDIC SolarWinds product and that they were in the process of conducting an internal review.

Also in December 2020, the National Security Agency (NSA) issued a Cybersecurity Advisory that nation state actors exploited a vulnerability in VMware products that allows attackers to forge security credentials and gain access to protected data.[70] The Cybersecurity Advisory recommended application of a vendor-issued patch. The FDIC

---

[63] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 2019).
[64] GAO, *Cybersecurity: Agencies Need to Fully Establish Risk Management Programs and Address Challenges*, GAO-19-384, (July 2019).
[65] U.S. House of Representatives, Committee on Financial Services, Subcommittee on Oversight and Investigations, Republican Staff Report, "*Securing the New Normal: An Examination of Cybersecurity Issues Related to Remote Work and the Transition to a Digital Supervisory Relationship* (Jan. 11, 2021); *see also* Jelena McWilliams, Chairman, Federal Deposit Insurance Corporation, *FDIC Response to House Committee on Financial Services Ranking Member's Request,* May 19, 2020 (reporting an increase in cyber threats associated with COVID-19 and FDIC actions to notify financial institutions and service providers critical to the banking industry).
[66] The Washington Post, *Russian Government Hackers are Behind a Broad Espionage Campaign That Has Compromised U.S. Agencies, Including Treasury and Commerce*, (December 14, 2020).
[67] The New York Times, *Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit*, (December 14, 2020).
[68] CISA, *CISA Issues Emergency Directive To Mitigate The Compromise Of SolarWinds Orion Network Management Products*, (December 13, 2020).
[69] CISA Cyber Activity Alert, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, (December 17, 2020); The New York Times, *Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit,* (December 14, 2020). Politico, *How Suspected Russian Hackers Outed Their Massive Cyberattack*, (December 16, 2020).
[70] NSA Cybersecurity Advisory, *Russian State-Sponsored Malicious Cyber Actors Exploit Known Vulnerability in Virtual Workspaces*, (December 7, 2020).

uses a VMware product, and FDIC officials represented that they took action to apply the patch and reduce the risk of exploitation for the FDIC VMware product.

In addition, the DHS recognized that "ransomware has rapidly emerged as the most visible cybersecurity risk playing out across our Nation's networks."[71] In a survey conducted by the data-protection firm Veritas, nearly 30 percent of Federal agency respondents reported that they were directly affected by ransomware attacks in the past 3 years. In addition, 80 percent of Federal respondents believe that ransomware and malware will be as great a concern—if not a greater concern—within the next 12 months.[72] We have work planned to review the FDIC's preparedness to handle a possible ransomware attack.

As of October 2020, the FDIC had 14 cloud-based systems. According to the GAO, cloud-based systems offer benefits but also pose cybersecurity risks.[73] For example, risks arise when agencies and cloud service providers fail to effectively implement security controls over cloud services. We have work planned to assess the FDIC's cloud solutions.

Enhancing the FDIC's Information Security Program and Practices

In our annual audit report, *The FDIC's Information Security Program- 2020* (October 2020), we identified 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. The weaknesses include:

- **Risk Management.** We found that the FDIC had not fully defined its Enterprise Risk Management governance, roles, and responsibilities.[74] In addition, the FDIC had not yet implemented recommendations to integrate privacy into its Risk Management Framework, nor did the FDIC always address Plans of Action and Milestones[75] in a timely manner.
- **Risk Acceptance Decisions Not Consistently Re-assessed.** We found that the FDIC did not consistently review its risk acceptance decisions or submit them to the FDIC's Authorizing Official for re-approval. As a result, the FDIC cannot effectively assess the level of risk it is incurring relative to established Risk Tolerance levels.
- **Unauthorized Software on the Network.** In May 2020, the FDIC found that an unauthorized commercial software application had been installed on 32 desktop workstations. The use of unauthorized software increases the risk of a security incident and the interruption to the safe operation of the FDIC's network and applications.
- **Privacy Control Weaknesses Not Fully Addressed.** The FDIC established a number of Data Protection and Privacy controls; however, it had not addressed 12 of

[71] DHS's CISA Insights, *Ransomware Outbreak*, (August 21, 2019).
[72] Veritas, *Ransomware Threats Is Your Agency Ready?*, (December 2019).
[73] GAO, *Cloud Computing Security, Agencies Increased Their Use of the Federal Authorization Program, but Improved Oversight and Implementation Are Needed*, GAO-20-126, (December 2019).
[74] See additional discussion of governance-related issues in Challenge 5 – Promoting and Aligning Strong Governance at the FDIC.
[75] A Plan of Action and Milestones is a management tool used by agency CIOs, security personnel, program officials, and others to track the progress of corrective actions pertaining to security vulnerabilities identified through security control assessments and other sources.

the 14 recommendations contained in our audit, *The FDIC's Privacy Program* (December 2019). These outstanding recommendations include, for example, monitoring employee and contractor compliance with policies for properly safeguarding sensitive electronic information; developing privacy plans for all information systems containing Personally Identifiable Information (PII)[76] consistent with OMB guidance; and implementing a privacy continuous monitoring program to regularly assess the effectiveness of privacy controls.

- **Oversight and Monitoring of Outsourced Systems Not Adequate.** We found that the FDIC had not properly categorized some of its outsourced information systems, or subjected these systems to a proper risk assessment, authorization to operate, and ongoing monitoring.
- **Cloud-based Systems Not Subject to Annual Control Assessments.** FDIC guidance requires security and privacy controls for cloud-based systems be assessed on a 3-year cycle, with at least some controls tested each year. However, we found that in two cases, the FDIC had not completed annual control assessments for more than 3 years after the FDIC authorized the systems to operate. Without annual control assessments, the FDIC cannot be sure that it will identify and remediate security and privacy weaknesses in a timely manner; these vulnerabilities may threaten the confidentiality, integrity, and availability of cloud-based systems.

We made eight recommendations to strengthen the effectiveness of the FDIC's information security program controls and practices. In addition, as of December 2020, there were 14 other unimplemented IT- and privacy-related recommendations from prior OIG reports.

In our audit report, *Security Controls Over the Federal Deposit Insurance Corporation's Regional Automated Document Distribution and Imaging System* (RADD) (June 2020), we assessed the effectiveness of selected security controls for protecting the confidentiality, integrity, and availability of the information in RADD against security controls in National Institute of Standards and Technology (NIST) guidance.[77] The RADD system contains over 5 million electronic records and serves as the official recordkeeping and electronic filing system for the FDIC's supervisory business records. We found that the FDIC's controls and practices in three security control areas were not fully effective, because either they did not comply with FDIC policy requirements or they were not implemented in a manner consistent with relevant NIST security guidance. The lack of documented roles, responsibilities, and procedures for audit logging caused the FDIC to be dependent upon the knowledge and experience of a limited number of staff. We made two recommendations for the FDIC to improve these security controls; these recommendations have been implemented.

FDIC IT systems are essential components of FDIC business processes. Absent effective IT security, the FDIC places the confidentiality, integrity, and availability of its information systems and data at risk.

---

[76] PII is any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, Social Security Number (SSN), date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information.

[77] The 8 NIST security control areas are: (1) Plans of Action and Milestones (POA&Ms), (2) Configuration Management, (3) Access Management, (4) Removable Media, (5) Encryption, (6) Audit Logging, (7) Security Authorization and Continuous Monitoring, and (8) Contingency Planning.

Challenge 4: Securing FDIC Personnel, Facilities, and Information

The FDIC is responsible for protecting a workforce of approximately 5,800 employees and 1,600 contract personnel who work at 94 FDIC facilities throughout the country. The FDIC should continue to strengthen its programs to ensure that its facilities are secure, that staff meet suitability requirements, and that the FDIC work environment is safe and free from discrimination and sexual harassment. The FDIC is also the custodian of 81 systems as well as hard-copy records containing sensitive information about banks and PII of employees, contractors, bank management, and bank deposit holders. The FDIC should control access to such information and maintain its security.

Based on an analysis conducted by Carnegie Mellon University, more than half of all Federal Government insider threats involved fraud.[78] Such incidents included the theft of PII for employees and non-employees, or sensitive Government databases. In most incidents, the individuals who stole the information had worked for their respective organization for more than 5 years and abused their privileged access.[79]

Federal agencies should have security measures in place to protect their people, property, and information. These security measures include processes to identify and assess individuals with criminal histories and questionable behavior.[80] The President's Management Agenda noted the importance of personnel security and suitability programs "to anticipate, detect, and counter both internal and external threats, such as those posed by trusted insiders who may seek to do harm to the Federal Government's policies, processes, and information systems."[81]

Further, Federal facilities should establish security measures commensurate with their internal and external risk[82] and have working environments that are free from discriminating, intimidating, hostile, or offensive behaviors. These behaviors can undermine an agency's mission by creating a hostile work environment that lowers productivity and morale, affects the agency's authority and credibility, and exposes the agency to litigation risk and costs.[83] Federal agencies also must safeguard and protect the privacy and sensitive data in their custody and possession.[84]

---

[78] Carnegie Mellon University, Software Engineering Institute, *Insider Threats in the Federal Government* (Part 3 of 9: Insider Threats Across Industry Sectors), (November 5, 2018).
[79] Carnegie Mellon University, Software Engineering Institute, *Insider Threats in the Federal Government* (Part 3 of 9: Insider Threats Across Industry Sectors), (November 5, 2018).
[80] GAO, *Key Issues: Government-wide Personnel Security Clearance Process – High-Risk Issue.*
[81] President's Management Agenda, *Security Clearance, Suitability/Fitness, and Credentialing Reform*.
[82] In 1995, President Clinton by Executive Order 12977 (October 19, 1995) created the Interagency Security Committee (ISC) in order to issue standards, policies, and best practices to enhance the quality and effectiveness of security in non-military Federal facilities in the United States.
[83] U.S. Merit Systems Protection Board Research Brief, *Update on Sexual Harassment in the Federal Workplace,* (March 2018) and 29 C.F.R. § 1604.11 (2015).
[84] In 2015 GAO expanded its Government-wide cybersecurity risk to include protecting the privacy of PII. See, GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 2019).

Improving the Effectiveness of the FDIC's Personnel Security and Suitability Processes

FDIC employees and contractors are subject to background investigations commensurate with the sensitivity of their positions, scope of responsibility, and access to classified National Security Information. The FDIC's Personnel Security and Suitability Program (PSSP) strives to ensure that FDIC employees and contractors have suitable character, reputation, honesty, integrity, and trustworthiness. A strong and effective PSSP reduces the risk of employee or contractor information breaches and identifies potential issues for the FDIC's Insider Threat Program.

In our OIG evaluation, *The FDIC's Personnel Security and Suitability Program* (January 2021), we assessed the effectiveness of the FDIC's PSSP. We determined that the FDIC's PSSP program was not fully effective in ensuring the timely completion of preliminary suitability screenings; background investigations commensurate with position risk designations; and re-investigations. Specifically, we found that:

- Four contractors with unfavorable background investigation adjudications continued to work at the FDIC from nearly 8 months to 5 years (until we notified the FDIC about these cases);
- The FDIC did not remove seven contractors with unfavorable adjudications in a timely manner;
- The FDIC did not follow its Insider Threat protocols and conducted limited risk assessments for contractors with unfavorable adjudications;
- The FDIC did not initiate numerous required periodic reinvestigations in a timely manner;
- Data on contractor position risks were unreliable;
- Employee background investigations were often not commensurate with position risk;
- The FDIC files were frequently missing some preliminary background investigation data; and
- The FDIC was not meeting its goals for completing preliminary background investigations within a specified timeframe.

We made 21 recommendations to strengthen PSSP controls and ensure the FDIC's compliance with Federal requirements. The FDIC should ensure that it satisfactorily addresses the risks associated with the PSSP, because the FDIC may increase hiring in response to the economic conditions caused by the current pandemic. As noted earlier, the FDIC Board approved an additional $261 million in contingency reserves in 2021 in order to ensure readiness for any potential increase in supervisory workload, bank failure activity, and administrative support.[85] A significant rise in hiring and use of contractors will dramatically increase the number of suitability screenings and background investigations processed through the FDIC's PSSP.

[85] *Proposed 2021 FDIC Operating Budget*, (December 1, 2020).

Sustaining a Work Environment Free from Discrimination, Harassment, and Retaliation

Sexual harassment within an organization can have profound effects and serious consequences for the harassed individual, fellow colleagues, and the agency as a whole. In certain instances, a harassed individual may risk losing a job or the chance for a promotion, and it may lead the employee to suffer emotional and physical consequences.

In our OIG evaluation, *Preventing and Addressing Sexual Harassment* (July 2020), we assessed the FDIC's sexual harassment-related policy, procedures, training, and practices for the period January 2015 through April 2019. We found that the FDIC had not established an adequate sexual harassment prevention program and should improve its policies, procedures, and training to facilitate the reporting of sexual harassment allegations and address reported allegations in a prompt and effective manner. Specifically, we found that the FDIC had not developed a sexual harassment prevention program that fully aligned with the five core principles promoted by the Equal Employment Opportunity Commission: (1) committed and engaged leadership; (2) strong and comprehensive harassment policies; (3) trusted and accessible complaint procedures; (4) regular, interactive training tailored to the audience and the organization; and (5) consistent and demonstrated accountability.

As part of our evaluation, we conducted a voluntary survey of FDIC employees. The survey responses provided insight into employee understanding of what constitutes sexual harassment, instances of sexual harassment experienced or observed at the FDIC, impediments to reporting, and the adequacy of training. Our survey found that approximately 8 percent of FDIC respondents (191 of 2,376) said that they had experienced sexual harassment at the FDIC during the period January 2015 to April 2019. Similarly, the Merit Systems Protection Board (MSPB) survey of FDIC employees, conducted in 2016 (based on data from 2014 to 2016), indicated that approximately 9 percent of FDIC respondents (40 of 427) had experienced sexual harassment. By comparison, the Government-wide average for Federal employees in this MSPB survey was 14 percent.

Although 191 FDIC respondents to the OIG survey reportedly experienced sexual harassment, the FDIC only received 12 reported sexual harassment allegations, including both formal complaints and misconduct allegations from January 2015 to April 2019. This response suggests that there may have been an underreporting of sexual harassment allegations.

Our survey further indicated that 38 percent of FDIC respondents who stated they had experienced sexual harassment said that they did not report the incident(s) for "fear of retaliation." Nearly 40 percent of FDIC respondents did not know, or were unsure of, how to report allegations of sexual harassment. Further, almost 44 percent of the FDIC respondents to the OIG survey felt that the FDIC should provide additional training on sexual harassment.

We made 15 recommendations to improve the FDIC's policies and procedures relating to the FDIC's actions in response to sexual harassment misconduct allegations; promote a culture in which sexual harassment is not tolerated and such allegations are promptly

investigated and resolved; ensure consistent discipline; and enhance training for employees and supervisors. At the time of this document, the FDIC had closed 2 of our 15 recommendations, and FDIC officials indicated that they are working towards addressing the remaining 13 recommendations.

Implementing Risk-Based Physical Security Management

In our OIG evaluation, *The FDIC's Physical Security Risk Management Process* (April 2019), we assessed whether physical security risk management processes met Federal standards and guidelines. We concluded that the FDIC had not established an effective physical security risk management process to ensure that it met Federal standards and guidelines.

We found that the FDIC did not conduct key activities in a timely or thorough manner for determining facility risk level, assessing security protections in the form of countermeasures, mitigating and accepting risk, and measuring program effectiveness. For example, for one of its medium-risk facilities, the FDIC began, but did not complete, an assessment more than 2½ years after the FDIC occupied the leased space. Collectively, these weaknesses limited the FDIC's assurance that it met Federal standards for physical security over its facilities. The FDIC completed the recommended actions from this report. We have work ongoing to assess whether the FDIC implemented effective controls to protect electrical power; heating, ventilation, and air conditioning; and water services at its Virginia Square office buildings.

Securing Sensitive and Personally Identifiable Information

In our OIG audit, *The FDIC's Privacy Program* (December 2019), we assessed the effectiveness of the FDIC's Privacy Program and practices by determining whether the FDIC complied with selected provisions in privacy-related statutes and OMB policy and guidance. We examined eight areas of the FDIC's Privacy Program and found that the FDIC faced challenges with respect to controls and practices in four areas. Specifically, the FDIC did not:

- Fully integrate privacy considerations into its risk management framework designed to categorize information systems, establish system privacy plans, and select and continuously monitor system privacy controls;
- Adequately define the responsibilities of the Deputy Chief Privacy Officer or implement Records and Information Management Unit responsibilities for supporting the Privacy Program;
- Effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII within established timeframes; and
- Ensure that Privacy Impact Assessments were always completed, monitored, published, and retired in a timely manner.

Weaknesses in the FDIC's Privacy Program increased the risk of PII loss, theft, and unauthorized access or disclosure, which could lead to identity theft or other forms of consumer fraud against individuals. In addition, weaknesses related to the management of Privacy Impact Assessments reduced transparency regarding the FDIC's practices for handling and protecting PII.

We made 14 recommendations intended to strengthen the effectiveness of the FDIC's Privacy Program and practices. These recommendations address the FDIC's need to implement information controls, monitor privacy controls, and complete policy and process documents. At the time of this writing, the FDIC has closed 3 of 14 recommendations and FDIC officials indicated that they were working towards addressing the remaining 11 recommendations.

In addition, in our OIG audit, *The FDIC's Information Security Program – 2019* (October 2019), we noted that the FDIC had not adequately controlled access to sensitive information and PII stored on its internal network and in hard copy. For example, we identified instances in which sensitive information stored on internal network shared drives was not restricted to authorized users.

We also conducted walkthroughs of selected FDIC facilities and found significant quantities of sensitive hard-copy information stored in unlocked filing cabinets and boxes in building hallways. We recommended that employees and contractor personnel properly safeguard sensitive electronic and hardcopy information. The FDIC has indicated that it secured the information identified by the OIG.

Mandatory telework at the FDIC increases the need for additional information security controls. As recognized by NIST, "[t]elework and remote access technologies often need additional protection because their nature generally places them at higher exposure to external threats compared to technologies that are only accessed from inside the organization."[86] Telework risks include a lack of physical security over mobile devices (such as laptops and tablets) and the use of unsecured network access.

The security and safety of FDIC personnel, facilities, and information is integral to the Agency's ability to execute its mission to maintain stability and public confidence in the Nation's financial system. The FDIC should have adequate safeguards in place to protect FDIC personnel, facilities, and information.

Challenge 5: Ensuring and Aligning Strong Governance at the FDIC

Effective governance is critical to ensure that the FDIC assesses risks and consistently implements its policies. The FDIC should ensure the establishment and proper function of its governance processes, including an Enterprise Risk Management (ERM) program. The pandemic demonstrated the importance of governance, and the need to quickly assess the risks to FDIC operations and make adjustments to its processes in order to maintain mission readiness. Quality data is also a critical component of FDIC governance to allow the Board, Executives, and Managers to assess the effectiveness of FDIC programs.

[86] NIST ITL Bulletin, *Security for Enterprise Telework, Remote Access, and Bring Your Own Device (BYOD) Solutions*, (March 2020).

Governance encompasses the ways in which an organization functions and how it is structured, overseen, managed, and operated.[87] A governance framework should ensure strategic guidance, effective monitoring of management by the board, and the board's accountability to stakeholders.[88]

The Federal Deposit Insurance Act[89] vests management of the FDIC to the FDIC Board. By statute, the FDIC Board is intended to consist of five members, all of whom are appointed by the President and confirmed by the Senate: the Comptroller of the Currency; the Director of the Bureau of Consumer Financial Protection; the FDIC Chairman and Vice Chairman; and another Appointive Director.[90] The FDIC Board has been operating with four members since 2015, and the Vice Chairman position has been vacant since April 2018.[91] Further, with the recent change in the Administration, the Board members from the Office of the Comptroller of the Currency and the Bureau of Consumer Financial Protection recently changed. Although the FDIC Board may delegate certain powers to officers of the FDIC, the FDIC Board members should exercise their oversight responsibilities, remain informed about FDIC activities, and review relevant documentation and financial statements.[92]

An important role for Board oversight is the Agency's ERM program.[93] ERM provides an entity-wide view of the full spectrum of internal and external risks to an organization.[94] An entity-wide assessment of risk allows boards and management to effectively allocate resources, prioritize and proactively manage risk, improve the flow of risk information to decision makers, and work towards successful accomplishment of their missions.

Data is the foundation for strong governance and an effective ERM program.[95] The FDIC should have accurate, reliable, and comprehensive data collection at each level of the organization in order to allow the Board, senior Executives, and Managers to monitor, oversee, and manage risk at the enterprise, as well as at the program level.

The pandemic presents unique challenges to the FDIC's ERM. For example, FDIC Board Members and Executives had to quickly identify and understand the many varied risks associated with the pandemic. These risks include those associated with the health, safety, and security of FDIC personnel and operations; the proper reconstitution

---

[87] American Bar Association, Business Law Today, *The Interplay Between Corporate Governance Issues and Litigation: What is Corporate Governance and How Does it Affect Litigation?,* (December 20, 2016).
[88] Organization for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance*, (2015).
[89] 12 U.S.C. § 1812(a)(1) (2019).
[90] 12 U.S.C. § 1812(a)(1) (2019); FDIC, *Bylaws of the FDIC*, (2018). Technically designated the Chairperson and Vice Chairperson in the statute and bylaws, it is longstanding FDIC practice to refer to the positions as Chairman and Vice Chairman. No more than three members of the Board may be from the same political party, and one member "shall have State bank supervisory experience."
[91] American Banker, *Pressure Grows on Administration to Fill Fed, FDIC Seats*, (November 3, 2019).
[92] Bylaws of the Federal Deposit Insurance Corporation, Adopted by the Board of Directors, (September 17, 2019); Wyoming Law Review, *Director Oversight and Monitoring: The Standard of Care and the Standard of Liability Post-Enron*, (2006).
[93] ERM is a governance issue that falls within the oversight responsibility of boards of directors. See Harvard Law School Forum on Corporate Governance and Financial Regulation, *Risk Management and the Board of Directors,* (March 20, 2018).
[94] Committee of Sponsoring Organizations of the Treadway Commission, *Enterprise Risk Management Integrating with Strategy and Performance,* (June 2017).
[95] Moody's Analytics, *Enterprise Risk Management: The Critical importance of Data*, (May 27, 2014).

of an office environment following an extended period of remote work; appropriate flexibilities for the workforce; a framework for the Agency's future protocols and culture to connect the organization; the effectiveness of the Agency's remote bank examinations and closures of failed banks; cybersecurity measures with personnel working remotely; capabilities to communicate in a virtual environment and use collaboration tools; and communications strategies for the Board's oversight of management and management's oversight of employees' work and performance.[96]

Aligning Enterprise Risk Management with Best Practices

According to OMB Circular Number A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, ERM is "an effective Agency-wide approach to addressing the full spectrum of the organization's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos."[97] The OMB requires that Federal agencies implement ERM to assist agencies in identifying, assessing, and mitigating internal and external risks.[98] Key components of ERM include: a Risk Appetite, Risk Tolerance, Risk Inventory, and Risk Profile.[99]

The FDIC Board appointed the FDIC's Operating Committee as the "focal point" for the coordination of risk management at the FDIC. The Operating Committee is comprised of Division and Office Directors and Deputies to the Chairman. The FDIC further designated the Operating Committee as the FDIC's Risk Management Council and the oversight body for ERM.[100]

In our OIG evaluation, *The FDIC's Implementation of Enterprise Risk Management* (July 2020) (ERM Report), we assessed the FDIC's implementation of ERM against relevant criteria and best practices. We reported that the FDIC needed to establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. Importantly, the FDIC did not clearly articulate in its policies and procedures how the Operating Committee, as the FDIC's designated Risk Management Council, performs its responsibilities. We also found that the FDIC had not clearly defined the roles, responsibilities, and processes of other risk committees and groups involved in ERM, including the FDIC Board.

As a result, we determined that ERM was not fully implemented at the FDIC, and, therefore, proper execution of program activities, roles, and responsibilities has yet to take place. Without a clear governance structure over ERM, the FDIC cannot ensure that ERM will fully mature and be integrated into the Agency and its culture. If ERM is

---

[96] Harvard Law School Forum on Corporate Governance, *COVID-19 and Corporate Governance: Key Issues for Public Company Directors,* (April 29, 2020); EY, *COVID-19: Five ways boards can help businesses improve their resilience*, (April 23, 2020).
[97] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control,* (July 15, 2016).
[98] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control*, (July 15, 2016).
[99] Risk Appetite is the risk an organization is willing to accept in pursuit of its mission; risk tolerance is the acceptable level of variance in performance relative to the achievement of objectives; risk inventory is a list of the risks facing the agency; and a risk profile is a prioritized inventory of significant risks identified and assessed by an agency through its risk assessment process.
[100] FDIC Directive 4010.3, *Enterprise Risk Management and Internal Control Program,* (October 25, 2018).

not fully matured and integrated into the Agency, there is a risk that the FDIC may not develop a comprehensive portfolio view of risk that would allow the FDIC to make efficient and effective decisions related to strategic planning, resource allocation, policy, and operations. We made eight recommendations to the FDIC to improve its ERM program. FDIC officials recently provided information indicating how the FDIC plans to address these recommendations, including revised Standard Operating Procedures. As of the date of this document, we are reviewing the information provided in order to assess whether the FDIC's proposed corrective actions align with our findings and satisfy the recommendations.

The ERM framework incorporates an agency's internal controls because controls are developed to mitigate risks.[101] As noted by the GAO in its FDIC financial statement auditor's report included in this Annual Report, the FDIC was found to have a significant internal control deficiency over financial reporting related to contract payment review processes. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. Without adequate contract payment review processes, the FDIC cannot reasonably assure that internal controls over contract payments are operating effectively, thereby increasing the risks that improper payments could occur and misstate the financial statements.

Additionally, another report reflects the need for the FDIC to instill ERM as part of the FDIC's culture and to ensure the full and comprehensive consideration of risks facing the Agency. In our evaluation report, *The FDIC's Personnel Security and Suitability Program* (January 2021), we found that the FDIC's ERM program did not fully address the level of risk in its Personnel Security and Suitability Program (PSSP). Specifically, we did not believe that the FDIC's risk assessment fully considered the various risks identified in our evaluation results, including operational, compliance, reporting, and reputational risks. For example, the FDIC was aware of programmatic failures to remove high-risk IT and armed guard contractors who had unfavorable adjudications. However, the FDIC did not integrate these programmatic shortcomings into its assessment of program risk.

On December 15, 2020, the FDIC announced an organizational change to make the Office of Risk Management and Internal Controls an independent office, and have the Chief Risk Officer report directly to the Deputy to the Chairman and Chief Financial Officer.

Ensuring and Maintaining Quality Data for Risk Oversight

FDIC Board members, Executives, and Managers need quality data to properly oversee the Agency and its Divisions, Offices, programs, and operations. Quality data should include at least the following five dimensions: accuracy, completeness, consistency, timeliness, and validity.

In several recent OIG reports, we found that FDIC systems data did not afford the FDIC with accurate, complete, reliable, and comprehensive data and information in order to effectively oversee Agency programs and operations.

[101] Committee of Sponsoring Organizations of the Treadway Commission, *FAQs for COSO Enterprise Risk Management – Integrated Framework.*

- *FDIC's Personnel Security and Suitability Program* (January 2021). We found that missing and inaccurate data impacted the ability of FDIC management to monitor the program. For example, FDIC systems did not contain preliminary approval dates and results for a total of 787 employees and contractors for the period from 1994 to 2019. Preliminary approval is required before the FDIC grants employees and contractors access to FDIC facilities and IT systems. We also found that FDIC systems did not accurately reflect contractors' position risk levels. Absent risk levels, the FDIC cannot ensure that it conducts appropriate background investigations for contractors employed at the FDIC.

- *Contract Oversight Management* (October 2019). We found that the FDIC was overseeing acquisitions on a contract-by-contract basis rather than on a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. In addition, we found that the FDIC's contracting system did not maintain certain key data in a manner necessary to conduct historical trend analyses, plan for future acquisition decisions, and assess risk in the FDIC's awarded contract portfolio. As a result, FDIC Board members and other senior management officials were not provided with a portfolio-wide view or the ability to analyze historical contracting trends across the portfolio, identify anomalies, and perform ad hoc analyses to identify risk or plan for future acquisitions.

In 2019, the FDIC launched an Enterprise Data Governance Initiative to assess the Agency's data quality and availability.[102] The FDIC also created a new Chief Data Officer position to lead the FDIC's data strategy. The Chief Data Officer will aim to develop and maintain the FDIC's data inventory and support the FDIC's move towards using artificial intelligence and machine learning.[103] The FDIC continues to work towards improving data quality at the Agency.

The FDIC relies on data to make mission-critical decisions from program assessments and staffing analytics to projections for bank failures and losses to the Deposit Insurance Fund. Absent quality data, the FDIC Board and its Executives, Managers, and staff may make decisions based on faulty or incomplete information. These decisions may impact the effectiveness of the FDIC's mission execution.

Timely Implementation of Corrective Actions

OIG audits and evaluations strive to prevent, deter, and detect waste, fraud, abuse, and mismanagement in the FDIC's programs and operations and to promote economy, efficiency, and effectiveness at the Agency. Our reports include recommendations addressed to FDIC management to address and mitigate program shortcomings, deficiencies, and vulnerabilities. In recent reports, we have noted instances where we found deficiencies or vulnerabilities in FDIC programs and operations that were similar to those identified in prior reports. These examples indicate that the previous corrective actions either were not sufficient to correct the underlying issues or were not supported and maintained over time. As a result, program deficiencies and vulnerabilities persist over many years.

---

[102] FDIC, *2019 Annual Report*.
[103] FDIC, *CIO Organization Strategic Plan 2020-2023: FDIC Business Challenges*.

- *The FDIC Personnel Security and Suitability Program* (January 2021). In our 2021 Report, we found that the FDIC's PSSP was not fully effective despite prior reports identifying similar program shortcomings and recommending comparable program changes. We found that the FDIC was still working to implement process changes to address findings from our 2014 evaluation report,[104] nearly 7 years ago. Specifically, we continued to identify repetitive problems with program data reliability, missing documentation, timeliness of processes, and a matching of background investigations with position risk. Our 2014 report included 10 recommendations to strengthen controls in program administration, oversight of contractor personnel, records management, and information systems reliability and controls. The FDIC closed these recommendations without further review by the OIG.[105] In 2013, the FDIC engaged a contractor to assess the status of the FDIC's PSSP, and the contractor found similar concerns related to lost and misplaced data, multiple systems that were not interconnected, and an inability to determine the status of contractor background investigations.

- *The FDIC's Implementation of Enterprise Risk Management* (July 2020). In our 2020 report, we found that the FDIC had not fully implemented an ERM program despite prior reports that identified and recommended program changes. Our 2020 evaluation was the third report within the last 13 years that included recommendations for the FDIC's implementation of an ERM program. In 2010, the FDIC engaged a consulting firm to evaluate its risk management practices. The consulting firm identified several gaps in the FDIC's risk management structure and recommended that the FDIC should establish a centralized, independent risk management organization; assign responsibility to the Chairman and Board of Directors to provide oversight of the Agency's risk management program; and develop comprehensive policies and guidelines to govern day-to-day risk management.

  Also, in 2007, we issued a report entitled, *The FDIC's Internal Risk Management Program* (November 2007), finding that the FDIC's approach to focus solely on internal risks was contrary to the ERM Framework. The report made seven recommendations intended to address the variances between FDIC practices and approaches and those advocated by the ERM Framework and applicable guidance; and to add clarity and structure to ERM. The FDIC, at that time, agreed with two of the seven recommendations and non-concurred with five recommendations.

- *The FDIC' Information Security Program—2020* (November 2020). We found that the FDIC had not addressed a recommendation made in our earlier report, *Audit of the FDIC's Information Security Program—2016*, to take appropriate steps to ensure that Data Communications Plans of Action and Milestones (POA&M) are addressed in a timely manner. A POA&M is a management tool used by agency Chief Information Officers, security personnel, program officials, and others to track the progress of corrective actions pertaining to security vulnerabilities identified through security control assessments and other sources.

[104] OIG Report, *The FDIC's Personnel Security and Suitability Program*, (August 2014).
[105] At that time, the FDIC closed recommendations without OIG review of the corrective actions. The OIG did not review all corrective actions before recommendations were closed. The OIG has since revised its processes, and the OIG now reviews all corrective actions to determine whether the FDIC's actions satisfy the recommendation and therefore it can be considered closed.

POA&Ms assist agencies in identifying, assessing, prioritizing, and monitoring the progress of corrective actions pertaining to security vulnerabilities. Open POA&Ms indicate that the FDIC has not completed action to remediate identified vulnerabilities.

Improved Oversight of IT Initiatives

IT governance provides organizations with a structured decision-making process underlying IT investment decisions and promotes accountability, due diligence, and the efficient and economic delivery of IT services.[106] When an organization does not maintain effective governance over its IT functions and operations, it can lead to negative results, including investments that do not align with the organization's mission, goals, or objectives; information systems that do not satisfy stakeholder needs; and IT projects that do not meet cost, schedule, or performance expectations.

In our report, *Governance of the FDIC's Mobile Device Management Solution* (December 2020), we assessed the adequacy of the FDIC's governance over a cloud-based mobile device management (MDM) solution to secure and manage smartphones and tablets. On October 4, 2019, the FDIC awarded a contract valued at $965,000, and in November 2019, the FDIC decided to terminate the contract, because the FDIC could not validate whether the MDM solution satisfied FDIC security requirements. Although the MDM project team coordinated with FDIC IT governance bodies, the Chief Information Officer Organization (CIOO) did not:

- Identify elevated and growing risks associated with the proposed MDM solution in reports describing the health and status of the project that were provided to CIOO Executives and other FDIC stakeholders;
- Resolve security concerns identified by the Office of the Chief Information Security Officer prior to procuring the proposed MDM solution; or
- Establish roles and responsibilities in its procedures for managing the use of Limited Authorizations to Operate (ATO).[107]

In addition to internal and contractor resources expended on the project, the FDIC compensated the vendor $343,533 for the proposed MDM solution. The FDIC never used the solution for which it had signed a contract to purchase. We made five recommendations to improve the FDIC's identification, assessment, and prompt reporting of project risks. By implementing our recommendation to require the concurrence of security and privacy officials before procuring new technologies, the FDIC can put $361,533 to better use.

In our OIG audit, *The FDIC's Governance of Information Technology Initiatives* (July 2018), we found that the FDIC faced a number of challenges and risks related to the governance of its IT initiatives. For example, the FDIC did not fully develop a

[106] See IT Governance Institute, *Board Briefing on IT Governance*, 2nd Edition. The IT Governance Institute is a nonprofit corporation that conducts research on global IT governance practices. The organization helps leaders understand how effective governance can assist in ensuring that IT supports business goals, optimizes IT-related business investment, and appropriately manages IT-related risks and opportunities.
[107] According to NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, (December 2018), Authorizing Officials may issue an ATO or an Interim Authority to Test when authorizing their information systems to operate. FDIC guidance refers to an Interim Authority to Test as a Limited ATO.

strategy to move IT services and applications to the cloud or obtain the acceptance of key FDIC stakeholders before taking steps to initiate cloud migration projects. The FDIC also had not implemented an effective Enterprise Architecture to guide the three IT initiatives we reviewed or the FDIC's broader transition of IT services to the cloud. The FDIC continues to work towards implementing one of our recommendations to identify and document IT resources and expertise needed to execute the FDIC's IT Strategic Plan.

The FDIC should ensure the establishment and proper function of its governance processes, including ERM. Effective governance allows the FDIC to assess and address risk and ensure consistent, nationwide, implementation of policies to fulfill the FDIC's mission. Quality data is a critical component to assess risk and measure the effectiveness of these governance activities. The FDIC should also ensure that corrective actions are taken and sustained to confirm that FDIC program weaknesses are remedied.

Challenge 6: Augmenting the FDIC's Sharing of Threat Information

Financial institutions and the FDIC both face a number of significant threats to their integrity, including the recent pandemic. Sharing threat information is critical to ensuring that banks and examiners have the necessary information to protect financial institutions, the banking sector, and the economy. Timely and actionable threat information allows bank management to mitigate risks and thwart dangers, and prompts the FDIC to adjust supervisory strategies in a timely fashion. Understanding the emerging threat landscape across all banks provides examiners with context to review a bank's processes. Also, threat information provides FDIC policy makers with perspective and context to adjust supervisory policies and examination procedures. Without effective threat information sharing, policy makers, bank examiners, and bank management may be unaware of threats that could affect the integrity, safety, and soundness of financial institutions.

The Cybersecurity and Infrastructure Security Agency identified consumer and commercial banking as a National Critical Function, defined as functions of the Government and private sector "so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety, or any combination thereof."[108] CISA further recognized funding and liquidity services as a National Critical Function as well.

A report by the Carnegie Endowment for International Peace identified numerous Information sharing gaps among the financial, national security, and diplomatic communities.[109] The report noted that financial regulatory authorities around the world

[108] DHS Cybersecurity and Infrastructure Security Agency, *National Critical Functions – An Evolved Lens for Critical Infrastructure Security and Resilience*, (April 30, 2019).
[109] Carnegie Endowment for International Peace, *International Strategy to Better Protect the Financial System Against Cyber Threats*, (November 18, 2020).

must regularly interact with law enforcement and national security agencies whose involvement is necessary to tackle cybersecurity threats.[110]

Collection and sharing of threat information is a key requirement to support National Critical Functions such as the banking system.[111] According to NIST guidance, the benefits of information sharing include: shared situational awareness, improved security posture, knowledge maturation, and greater defensive agility.[112] Information sharing also allows organizations to leverage "knowledge, expertise, and capabilities … to gain a more complete understanding of threats" and allow for threat-informed decision making.[113] Further, multiple sources of threat information can allow an organization to enrich existing information and make it actionable. NIST guidance also recognized that threat information sharing should be multi-directional among Federal agencies and respective private-sector stakeholders.[114]

In its Annual Report for 2020, FSOC recognized the critical importance of sharing threat information with the Financial Services Sector and among Federal Government agencies.[115] Further, in its report, *Semiannual Risk Perspective* (Spring 2020), the OCC encouraged banks to monitor information provided by law enforcement and international organizations regarding the "ways criminals are adapting scams and money laundering techniques to exploit vulnerabilities created by the pandemic."[116]

Threat information about money laundering is particularly important to banks, because the Bank Secrecy Act requires that banks help Government agencies detect and prevent money laundering by, among other things, having effective compliance programs to monitor and report suspicious activities. FinCEN recently issued an advisory to banks to encourage information sharing related to transactions that may involve terrorist financing or money laundering.[117] Specifically, the advisory provided banks with potential indicators of ransomware and money laundering activities because of the critical role banks play in the collection of ransomware payments.

The FDIC's Sharing of Threat Information with Banks

Banks are required to have "a means to collect data on potential threats that can assist management in its identification of information security risks."[118] Threat information allows banks to combat and mitigate threats.[119] Also, since threat actors often attack more than one organization in an industry, information sharing among organizations in a

---

[110] Carnegie Endowment for International Peace, *International Strategy to Better Protect the Financial System Against Cyber Threats*, (November 18, 2020).
[111] DHS defines a threat as "a natural or man-made occurrence, individual, entity, or action that has or indicates the potential to harm life, information, operations, the environment and/or property." DHS, *DHS Risk Lexicon*, (September 2008). DHS Cybersecurity and Infrastructure Security Agency, *National Critical Functions – An Evolved Lens for Critical Infrastructure Security and Resilience*, (April 30, 2019).
[112] NIST, Special Publication 800-150, *Guide to Cyber Threat Information Sharing*, (October 2016).
[113] NIST, Special Publication 800-150, *Guide to Cyber Threat Information Sharing*, (October 2016).
[114] NIST, Special Publication 800-150, *Guide to Cyber Threat Information Sharing,* (October 2016).
[115] FSOC*, 2020 Annual Report.*
[116] OCC, *Semiannual Risk Perspective*, (Spring 2020).
[117] Financial Crimes Enforcement Network, *Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments*, (October 1, 2020).
[118] FFIEC, Business Continuity Planning Booklet, *Risk Assessment*, (available on the FFIEC website).
[119] FS-ISAC, *Threat Information Sharing and GDPR: A Lawful Activity that Protects Personal Data*.

particular sector, in real time, may warn other entities and allow them to address and mitigate vulnerabilities.[120]

Federal law required the Director of National Intelligence and other Federal agencies to issue procedures to facilitate and promote threat information sharing.[121] In February 2016, procedures were outlined for Federal agencies to share unclassified and classified cybersecurity information with non-Federal entities, such as financial institutions.[122] These procedures require that Federal Government agencies make every reasonable effort to share cyber threat information on a timely basis. When threat information is classified, the procedures encourage Federal agencies to "downgrade, declassify, sanitize or make use of tearlines to ensure dissemination of threat information to the maximum extent possible."[123]

The Federal Financial Institutions Examination Council (FFIEC)[124] recommends that financial institutions should receive threat information from multiple sources. For example, the FFIEC recommends that banks join the Financial Services Information Sharing and Analysis Center (FS-ISAC). ISACs serve as a central resource for member organizations to gather and exchange cyber-threat information. Financial institutions are encouraged to use FS-ISAC and other resources to "monitor cyber threats and vulnerabilities and to enhance their risk management and internal controls."[125] The FFIEC also encourages banks to collect and gather information from the FBI, the Cybersecurity and Infrastructure Security Agency, and the U.S. Secret Service Cyber Fraud Task Force.[126]

FDIC examination guidance requires that examiners evaluate banks' processes for obtaining and assessing threat information. Examiners may face challenges in assessing whether the threat information received by a bank is sufficient to assess the effectiveness of banks' threat identification and mitigation processes if banks do not receive information from FFIEC-recommended sources.

---

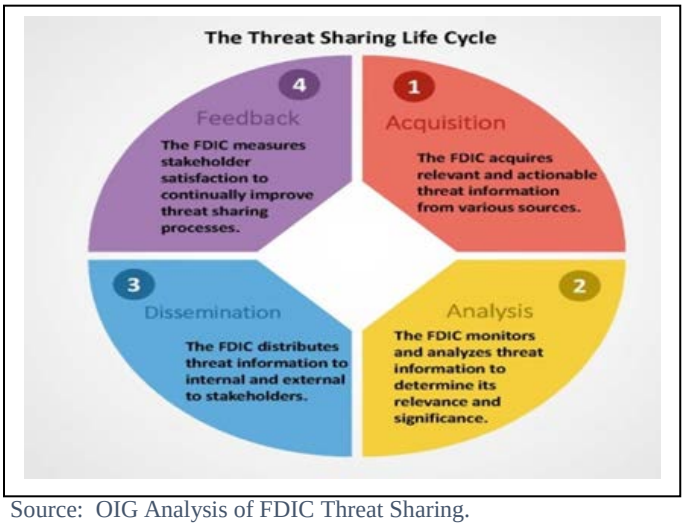
[120] FS-ISAC, *Threat Information Sharing and GDPR: A Lawful Activity that Protects Personal Data*.
[121] The Cybersecurity Information Sharing Act (2015).
[122] Office of the Director of National Intelligence, DHS, Department of Defense, and Department of Justice, *Sharing of Cyber Threat Indicators and Defensive Measures by the Federal Government under the Cybersecurity Information Sharing Act of 2015*, (February 16, 2016).
[123] Intelligence Community Directive 209, *Tearline Production and Dissemination*, (September 6, 2012), defines tearlines as "portions of an intelligence report or product that provide the substance of a more highly classified or controls report without identifying sensitive sources, methods, or other operational information."
[124] The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The Council is an interagency body empowered to prescribe uniform principles, standards, and report forms for the Federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration, the OCC, and the Bureau of Consumer Financial Protection and to make recommendations to promote uniformity in the supervision of financial institutions. FFIEC, *Cybersecurity and Threat and Vulnerability Monitoring and Sharing Statement*, (November 3, 2014).
[125] FFIEC, *Cybersecurity and Threat and Vulnerability Monitoring and Sharing Statement*, (November 3, 2014).
[126] See FFIEC, *Cybersecurity and Threat and Vulnerability Monitoring and Sharing Statement*, (November 3, 2014). Banks can connect to the FBI's Infraguard system in a partnership between the FBI and the private sector to provide, among other things, information sharing. The Cybersecurity and Infrastructure Security Agency provides alerts and education concerning cybersecurity. The U.S. Secret Service Cyber Fraud Task Force aims to improve information sharing and best practices on investigations of financially motivated cybercrime.

Creating a Framework to Share Threat Information with Examiners and Policy Makers

The key to the exchange of threat information is establishing and implementing a framework for sharing threat information. As shown in Figure 2, we identified four phases of a threat information sharing framework based upon a review of the best practices from Government and other authoritative sources.

It is important that examiners and policy makers are aware of threats facing financial institutions to identify gaps in banks' threat analyses and to adjust examination policies for emerging threats.

Figure 2: Threat Sharing Lifecycle at the FDIC



Source: OIG Analysis of FDIC Threat Sharing.

Certain FDIC staff at Headquarters have access to specific threat information held by the U.S. Government, and much of the information is confidential and sensitive. The FDIC, however, should have procedures in place to share such threat information effectively. Without formal processes, the FDIC cannot assess whether it is appropriately acquiring, analyzing, and disseminating timely threat information to banks and to FDIC examiners and policy makers.

Absent a threat information sharing framework, the FDIC leaves threat information acquisition, analysis, dissemination, and feedback to the discretion of a limited number of employees. In addition, it is important that staff charged with threat sharing responsibilities have received the proper guidance, procedures, background, and training to conduct thorough analysis of the information, assess the risks to financial institutions, and disseminate the information to other FDIC personnel who need to know.

Moreover, the FDIC faces challenges in transmitting relevant information from classified sources to key examiners and policy makers in Regional and Field Offices. In order to access, store, and handle classified information, FDIC policy makers and examiners either must have relevant security clearances and secure facilities—or alternatively, the FDIC must have processes in place to distribute similar information that is available in an unclassified format to policy makers and examiners. We have work ongoing to assess the effectiveness of the FDIC's threat sharing efforts.

Limited Requirements for Banks to Report Cyber Threats

The FDIC should be aware of cyber incidents targeted towards insured banks. For example, we identified two instances in which FDIC-supervised financial institutions fell victim to ransomware attacks but did not notify the FDIC. In one instance, the FDIC did not learn about the attack until state examiners discovered it during an examination. In the second instance, the FDIC did not learn about the attack until after the institution

disclosed it in a Suspicious Activity Report (SAR) filed with FinCEN. While these mechanisms may provide information about cyberattacks, they are not designed to ensure prompt and timely notification to the FDIC (or other primary federal regulators) about cyber incidents affecting the safety and soundness of institutions.[127]

In addition, threats are rarely specific to one organization.[128] The Federal Reserve Bank of Boston's Cyber Threat Sharing Forum notes that "a malicious actor often uses the same tactics and techniques that they've used to attack one financial institution on the next, and so on."[129] A threat to one bank also has the potential to affect numerous banks through interconnected systems, such as shared TSPs.

The *Interagency Guidelines Establishing Information Security Standards*[130] (Interagency Guidelines) state that every financial institution should develop and implement a Response Program to address incidents of unauthorized access to customer information whether at the bank or the institution's TSP.[131] According to the Interagency Guidelines and supplemental guidance, an institution's Response Program should include procedures for "notifying its primary Federal regulator as soon as possible when the institution becomes aware of an incident involving unauthorized access to or use of sensitive customer information." However, this reporting requirement applies only to incidents that compromised customer information. Federal regulations did not address reporting to Federal bank regulators for other types of destructive cyber incidents that could jeopardize the safety and soundness of an institution. Further, the FFIEC recommended, but Federal regulators did not require, that financial institutions that were victims of cyberattacks involving extortion notify their primary regulator.[132]

On April 30, 2020, we issued a Management Advisory Memorandum to the FDIC noting the absence of a Federal requirement for banks to promptly report instances of disruptive or destructive cyber incidents to Federal banking regulators. Such a requirement would provide the FDIC and other Federal banking regulators consistent information to assess threats and implement supervisory actions in a timely manner. This information would also assist the FDIC in its role as receiver for failed financial institutions, as it would allow for timely preparation for a potential resolution especially as cyberattacks can rapidly impact a bank's operations.

---

[127] Institutions are required to file a SAR within 30 calendar days following initial detection of facts triggering the SAR filing requirement. The SAR filing deadline may be extended an additional 30 days (up to a total of 60 calendar days) if no suspect is identified. 12 C.F.R. § 353.3.

[128] American Bar Association, SciTech Lawyer, *Threat Sharing Under GDPR*, (Spring 2019).

[129] Federal Reserve Bank of Boston, *Cyber-threat Sharing Forum Fosters Open Dialogue, Non-competitive Environment, Financial Services Organizations Share Information to Thwart Cybercrime*, (October 24, 2017).

[130] Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice, Part 364, App. B (Supp. A). The FDIC, OCC, Board of Governors of the Federal Reserve System (FRB), and former Office of Thrift Supervision (OTS) issued this supplemental guidance to interpret the requirements of section 501(b) of the Gramm-Leach-Bliley Act and the Interagency Guidelines. The Interagency Guidelines are promulgated by the FDIC, OCC, FRB, and former OTS. The FDIC published the Interagency Guidelines for the entities subject to its jurisdiction in 12 CFR Part 364, App. B and 12 CFR Part 391, subpart B, App. B.

[131] 12 CFR Part 364 defines customer information as any record containing non-public personal information about a customer that is maintained by or on behalf of the institution.

[132] FFIEC Joint Statement, *Cyber Attacks Involving Extortion,* (November 2015).

In response to our Management Advisory Memorandum, on December 15, 2020, the FDIC, Department of the Treasury, and Federal Reserve issued a notice of proposed rulemaking requiring banks to notify their primary banking regulator of computer-security-related incidents.[133] The proposed rule requires that banks report an incident "as soon as possible and no later than 36 hours after the banking organization believes in good faith that the incident occurred." Further, the proposed rule would require that TSPs notify affected banking organizations immediately when the TSP experiences computer security incidents that materially disrupt, degrade, or impair provided services.

The sharing of threat information enhances the resiliency of the banking sector by allowing bank management to identify and thwart threats. The FDIC should ensure that banks, examiners, and policy makers receive timely and actionable threat information to mitigate threats and to adjust supervisory strategies to address emerging risks.

Challenge 7: Supporting Diversity in Banking

Access to the financial system by minority communities is vital to fostering economic prosperity. Minority communities and businesses have suffered significantly during the pandemic. The FDIC plays an important role to support Minority Depository Institutions that serve and promote minority and low- and moderate-income communities. This work can be enhanced with the FDIC's continued commitment to diversity and inclusion in the Federal regulatory process, which is critical for the FDIC to foster greater financial inclusion for all Americans.

Federal financial regulators can influence economic inclusion through their support of Minority Depository Institutions (MDI).[134] MDIs promote the economic viability of minority and underserved communities and foster financial inclusion by expanding credit to give more Americans the opportunity to build businesses, afford higher education, achieve homeownership, and create strong, vibrant communities.[135]

Minority-owned businesses have been disproportionately affected by the pandemic. According to a study by the Federal Reserve Bank of New York (FRB-NY), the number of active small businesses fell by 22 percent between February and April 2020. African American businesses suffered a 41-percent drop, Latinx businesses fell by 32 percent, and Asian businesses decreased by 26 percent.[136]

---

[133] Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 2299 (January 12, 2021).
[134] MDIs include Federally-insured depository institutions where 51 percent or more of the bank's voting stock is owned by minority individuals who are citizens or permanent legal residents of the United States; and/or a majority of the institution's Board of Directors is minority and the community that the institution serves is predominantly minority.
[135] cnbc.com, *Black Families have 10 times less wealth than whites and the gap is widening – here's why* (December 19, 2018); *see also* McKinsey & Co., *The case for accelerating financial inclusion in black communities*, (February 25, 2020).
[136] Federal Reserve Bank of New York, *Double Jeopardy: COVID-19's Concentrated Health and Wealth Effects in Black Communities*, (August 2020).

In addition, according to the FRB-NY, the Federal Government's PPP loans designed to assist small businesses reached only 20 percent of eligible companies in states with the highest numbers of African American-owned businesses.[137] The FRB-NY stated that this coverage gap is the result of minority businesses lacking established banking relationships or representing only a small portion of community banks' market share.[138] Such disparities emphasize the role financial regulators play in influencing and enhancing financial inclusion for all Americans through the requirements of the Community Reinvestment Act (CRA)[139] and fulfilling the goals of the Financial Institutions Reform, Recovery, and Enforcement Act of 1989 (FIRREA).[140]

The FDIC's activities in support of FIRREA include facilitating partnerships to provide outreach, technical assistance, education, and training to MDIs; encourage the creation of new MDIs; facilitate the preservation of the minority character if an MDI fails; and advocate for MDIs through research and highlighting the important role these banks play in their communities. The CRA is intended to encourage financial institutions to help meet the credit needs of the communities in which they operate, including low- and moderate-income neighborhoods, consistent with safe and sound banking operations.

Also, members of minority communities face challenges in accessing banking services. The FDIC Chairman noted that:

> Despite meaningful improvements in recent years, the rates for black and Hispanic households who do not have a checking or savings account at a bank remain substantially higher than the overall 'unbanked' rate. Similarly, black and Hispanic households are less likely to have mainstream credit (*i.e.*, credit products that are likely reported to credit bureaus) across all income levels. And savings rates remain lower among these households, which results in greater difficulty dealing with unexpected expenses.[141]

The FDIC recognized the importance of expanding access to quality financial services. In a 2019 study, *How America Banks: Household Use of Banking and Financial Services*, the FDIC found that 5.4 percent (about 7.1 million) of U.S. households lacked a checking or savings account at an insured financial institution.[142] This was the lowest unbanked rate since the survey began in 2009. Minority households were more likely to be among the unbanked. For example, 13.8 percent of Black households and 12.2 of Hispanic households were unbanked in 2019 compared to 2.5 percent of White households.

Notwithstanding this improvement, the FDIC predicted that the rapid and dramatic increase in the unemployment rate due to the pandemic will result in an increase in the

---

[137] Federal Reserve Bank of New York, *Double Jeopardy: COVID-19's Concentrated Health and Wealth Effects in Black Communities*, (August 2020).
[138] Federal Reserve Bank of New York, *Double Jeopardy: COVID-19's Concentrated Health and Wealth Effects in Black Communities*, (August 2020).
[139] 12 U.S.C. 2901, *et seq*.; *see also* 12 C.F.R. Parts 25, 228, 345, and 195 (implementing regulations).
[140] *See FDIC Policy Statement Regarding Minority Depository Institutions*, 67 Fed. Reg. 18620 (April 16, 2002).
[141] Jelena McWilliams, FDIC Chairman, Keynote speech before the University of Chicago Law School and American Financial Exchange Webinar on *The Role of Minority Depository Institutions and Innovation in the Age of COVID-19, Creating a Financial System of Inclusion and* Belonging, (August 26, 2020).
[142] FDIC, *How America Banks: Household Use of Banking and Financial Services – 2019 FDIC Survey*.

unbanked rate from its level just before the pandemic.[143] This forecast was based upon two considerations: (1) changes in the socioeconomic circumstances of U.S. households have contributed to changes in the unbanked rate; and (2) the unbanked rates have been higher among certain segments of the population, including lower-income households, unemployed households, and households with volatile income. From the peak of the unbanked rate in 2011 to the lowest unbanked rate in 2019, approximately two-thirds of the decline was associated with improvements in the socioeconomic circumstances of U.S. households. Relevant to the current economic conditions resulting from the pandemic, the FDIC noted in its most recent unbanked Americans report that a recent disruption resulting in significant income loss or job loss is a contributing event resulting in households becoming unbanked.[144]

Supporting Minority Depository Institutions

MDIs play a vital role in assisting minority and under-served communities. MDIs are resources to foster the economic viability of these communities by providing banking and credit services. The primary challenge for the FDIC is to measure the effectiveness of its efforts in supporting MDIs, including the assistance provided to under-served, unbanked, and underbanked communities.

The FDIC plays an important role in preserving and promoting MDIs. In our report, *Minority Depository Institution Program at the FDIC* (September 2019), we reviewed the FDIC's actions to preserve and promote MDIs and assessed achievement of the MDI Program goals. We found that 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.

However, the FDIC did not evaluate the effectiveness of some 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 they provide. We further found that FDIC Headquarters did not define the types of activities that it considered to be technical assistance, as distinct from training, education, and outreach events. In addition, 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. The FDIC implemented changes in response to our five recommendations.

As part of its program changes and in response to our OIG report, on August 21, 2020, the FDIC Board approved *Proposed Revisions to its Statement of Policy Regarding Minority Depository Institutions*. Through these Proposed Revisions, the FDIC indicated its intent to establish new requirements to measure the effectiveness of the MDI

[143] FDIC, *How America Banks: Household Use of Banking and Financial Services – 2019 FDIC Survey*, (reporting that the FDIC 2013 survey of unbanked Americans found that one in three households (34.1 percent) that became unbanked in the prior 12 months experienced either a significant income loss or a job loss that contributed to their becoming unbanked).
[144] FDIC, *How America Banks: Household Use of Banking and Financial Services – 2019 FDIC Survey*.

program. The FDIC also stated that it has taken additional steps to increase MDI representation on the FDIC Community Bank Advisory Committee (CBAC);[145] established a new CBAC subcommittee to focus on the work of MDIs;[146] and enabled MDIs to review potential purchases of a failing MDI before non-MDI institutions have an opportunity to consider such purchases.[147] We have not yet reviewed the effectiveness of these changes to the MDI program, but will continue to monitor the FDIC's efforts to support its MDI program.

Ensuring Minority Representation Among Policy Makers

Federal financial regulators determine public policy, mindful of an array of considerations, including the allocation and cost of capital, public interest over narrower investor interests, protecting a diverse public that necessitates clear disclosures for individuals from differing backgrounds, and determining who is eligible to receive Government assistance in times of economic distress. At times, Federal regulatory policy has been made without the benefit of minority representation at the decision-making table.[148] For example, according to an analysis from the Georgetown University Law Center, African Americans represented 3 percent (10 of 327) of Federal financial regulatory appointments requiring Senate confirmation.[149] As of July 2020, there was one African American appointee among 21 financial regulators.[150] Further, about 4 percent (5 of 120) of Federal regulatory senior policy staff is African American – in comparison to 13.4 percent of the overall U.S. population.[151] A study by the Brookings Institution stated that "[t]he absence of African American financial regulators poses enormous challenges from the standpoint of participatory democracy and economic inclusion."[152]

At the FDIC, the Chairman recently testified that within the Agency's entire workforce, minorities represented over 30 percent of permanent employees (as of the end of 2019).[153] In 2019, the FDIC permanent and non-permanent workforce included more

---

[145] *See* *FDIC Advisory Committee on Community Banking*. The FDIC's Advisory Committee on Community Banking MDI Subcommittee members represent a diverse range of MDIs, including African American, Hispanic, Asian American, and Native American institutions differing in business model, size, and location. The nine members of the MDI Subcommittee represent about 20 percent of all 96 MDIs supervised by the FDIC.

[146] *See* *MDI Subcommittee to FDIC's Advisory Committee on Community Banking.* The new MDI Subcommittee is intended to provide feedback on the FDIC's strategies in fulfilling its five statutory goals for MDIs (as required by Section 308 of FIRREA), to promote collaboration, partnerships and best practices; and to identify ways to highlight the work of MDIs in their communities.

[147] Testimony of FDIC Chairman Jelena McWilliams before the Senate Committee on Banking, Housing, and Urban Affairs on *Oversight of Financial Regulators*, (November 10, 2020).

[148] Brookings Institution, *The Absence of Black Financial Regulators*, (September 2, 2020).

[149] The Georgetown University Law Center, *What do the Data Reveal about (the Absence of Black) Financial Regulators?*, (July 20, 2020).

[150] The Wall Street Journal, *Black Regulators Rarely Appointed to Oversee Wall Street*, (July 21, 2020).

[151] The Georgetown University Law Center, *What do the Data Reveal about (the Absence of Black) Financial Regulators?*, (July 20, 2020).

[152] Brookings Institution, *The Absence of Black Financial Regulators*, (September 2, 2020).

[153] Testimony of FDIC Chairman Jelena McWilliams before the Senate Committee on Banking, Housing, and Urban Affairs on *Oversight of Financial Regulators*, (November 10, 2020); *see also* Statement of Nikita Pearson, Acting Director, Office of Minority and Women Inclusion, Federal Deposit Insurance Corporation on *Holding Financial Regulators Accountable for Diversity and Inclusion: Perspectives from the Offices of Minority and Women Inclusion*, before the Subcommittee on Diversity and Inclusion of the Committee on Financial Services, U.S. House of Representatives (September 8, 2020).

than 17 percent Black American, 4 percent Hispanic American, 6 percent Asian American, 0.6 percent American Indian or Alaska Native, and 1.7 percent for individuals of two or more races. Among the FDIC's Executive Managers, Black Americans represented 12.3 percent, Asian Americans 2.2 percent, Hispanic Americans represented 1.4 percent, and 0.7 percent of Executives were American Indian or Alaska Native.[154]

In our OIG report, *The FDIC's Efforts to Provide Equal Opportunity and Achieve Senior Management Diversity* (November 2014), we assessed the Agency's operations and efforts to provide equal opportunity for minorities and women to obtain senior management positions. We reported the underrepresentation of female, Hispanic, and Asian FDIC employees at the Executive Manager (EM) level as compared to the Federal Senior Executive Service (SES) workforce. Specifically, 28 percent of EMs at the FDIC were female, but the population of female executives across Federal agencies was 34 percent; 2 percent of FDIC EMs were Hispanic versus 4 percent across Federal agencies; and 2 percent of FDIC EMs were Asian while the Federal SES Asian population was 3 percent. The FDIC addressed the nine recommendations in this report.

According to the FDIC, as of November 2020 EM representation now includes 37 percent female, 3.9 percent Hispanic, and 5.5 percent Asian. According to FDIC officials, in 2021, the FDIC will announce the first FDIC Performance Goal dedicated to improving diversity, equity, and inclusion. Also, the FDIC has recently implemented a new performance standard for managers that focuses on cultivating an inclusive, harassment-free work environment.

The FDIC plays an important role in supporting and empowering minority communities' access to capital. The FDIC should continue to assess its MDI supervisory and outreach programs to encourage and preserve MDIs. Also, the FDIC should continue its efforts to enhance diversity and inclusion among senior decision makers to ensure that multiple viewpoints are considered in its policy making decisions.

[154] FDIC, Office of Minority and Women Inclusion, *Section 342 Dodd-Frank Wall Street Reform and Consumer Protection Act Report to Congress* (2019) (FDIC-07-2020).

Challenge 8: Managing Human Resources and Planning for the Future Workforce

The FDIC has approximately 5,800 employees in six Regional Offices across the country, and 42 percent of FDIC employees (nearly 2,400 individuals) are eligible to retire within 5 years. The FDIC faces retirement rates of almost 60 percent for FDIC Executives and Managers over that same time period. The FDIC should continue to manage the agency's exposure to gaps in leadership and mission-critical skills, especially given the significant investments in, and time required for, bank examiner commissioning.

Approximately 15 percent of the nearly 2.1 million Federal workforce are reportedly eligible to retire.[155] In March 2019, the GAO recognized strategic human capital management as a continuing Government-wide area of high risk.[156] The GAO identified the need for Federal agencies to measure and address existing mission-critical skill gaps, and to use workforce analytics to predict and mitigate future gaps.[157] A lack of strategic workforce planning may have lasting effects on the capacity of an agency's workforce and its ability to fulfill its mission.[158]

Over the next 5 years, through 2025, approximately 42 percent of current FDIC employees will be eligible to retire, and approximately 60 percent of current FDIC Executives and Managers will be eligible to retire. Without proper strategies to plan for succession and to manage turnover, these retirements can result in organizational gaps in knowledge, experience, and leadership.[159] Also, retirements could impact skills gaps for specialized positions such as bank examiners.[160]

On March 5, 2020, the FDIC Chairman announced a voluntary separation incentive and early retirement program intended to "increase the agility and effectiveness of the FDIC workforce, and to ensure that we can appropriately transition the skills, tools, and leadership necessary to fulfill mission-critical readiness."[161] According to the FDIC, the program could facilitate orderly succession management by providing the Agency with an opportunity to accelerate its transition to new skills, tools, and leadership that will be needed in the future to fulfill the FDIC's mission responsibilities.

---

[155] FedWeek, *Retirement Wave? Eligibility Numbers Holding Steady*, (January 7, 2020).
[156] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 2019).
[157] GAO, *High-Risk Series: Substantial Efforts Needed to Achieve Greater Progress on High-Risk Areas*, GAO-19-157SP, (March 2019).
[158] GAO, *Federal Workforce: Key Talent Management Strategies for Agencies to Better Meet Their Missions*, GAO-19-181, (March 2019).
[159] GAO, *Federal Workforce: Sustained Attention to Human Capital Leading Practices Can Help Improve Agency Performance*, GAO-17-627T, (May 2017).
[160] GAO, *Human Capital: Improving Federal Recruiting and Hiring Efforts*, GAO-19-696T, (July 2019).
[161] Memorandum from Chairman McWilliams to FDIC Employees, *Reshaping the FDIC for the Future and Improving Our Preparedness*, (March 5, 2020).

On March 16, 2020, however, the program was suspended so that the Agency could assess the impact of the pandemic on the banking industry. In October 2020, the Chairman stated that "[a]ny decision to implement [the separation incentive or early retirement program] in 2021 would likely target a much smaller group of employees as the Agency continues to respond to the pandemic."[162]

Assessing Potential Retirement Waves in the FDIC's Primary Divisions

The FDIC must continue to manage the Agency's exposure to personnel retirements in key divisions. Although the FDIC's overall retirement-eligible population is 42 percent, five key Divisions have staff retirement-eligible rates ranging from 44 to 68 percent. Absent proper management, retirements may lead to gaps in leadership and mission-critical skills, especially given the significant investments in, and time required for, bank examiner commissioning.

Approximately 93 percent of all FDIC employees work in one of the FDIC's nine primary and support Divisions. As shown in Table A, 30 to 68 percent of the FDIC staff in these Divisions are eligible to retire in the next 5 years. Notably, all nine FDIC Divisions have retirement eligibility rates that are higher than the Federal Government-wide rate of 15 percent.

Table A: Retirement Eligibility Statistics for Key FDIC Divisions

Division	Staff Eligible to Retire in 2025	Executives and Managers Eligible to Retire in 2025
Division of Resolutions and Receiverships (DRR)	68 percent	66 percent
Division of Finance (DOF)	55 percent	75 percent
Legal Division	55 percent	52 percent
Division of Administration (DOA)	56 percent	64 percent
Division of Information Technology (DIT)	44 percent	39 percent
Division of Risk Management Supervision (RMS)	39 percent	68 percent
Division of Complex Institution Supervision & Resolutions (CISR)	35 percent	28 percent
Division of Depositor and Consumer Protection (DCP)	34 percent	57 percent
Division of Insurance and Research (DIR)	30 percent	48 percent

Source: OIG analysis of FDIC-provided data as of June 1, 2020.

Division Executives and Managers have retirement eligibility rates ranging from 28 to 75 percent. For instance, approximately 75 percent of Executives and Managers within DOF are eligible to retire in the next 5 years. DOF staff manages the liquidity of the Deposit Insurance Fund to ensure that money is available to the DRR to pay depositors quickly in the event of a bank failure, and attorneys in the Legal Division assist the DRR in structuring resolution agreements.

Similarly, approximately 66 percent of Executives and Managers in the DRR and approximately 68 percent of Executives and Managers in the RMS can retire within the same timeframe. DRR staff is responsible for managing failed bank resolutions and

[162] Chairman's Town Hall Teleconference (October 7, 2020).

receiverships, including ensuring the prompt payment of deposit insurance funds to eligible bank customers. Absent seasoned professionals with knowledge of lessons learned from past crises, the FDIC may not be sufficiently agile in executing resolution and receivership activities in future bank failures. The FDIC faces significant risks regarding retirement eligibility in key Divisions that support crises readiness efforts.

As recognized by the GAO, retirement waves may result in leadership gaps.[163] The 5-year retirement eligibility rates of Executives and Managers presents a risk that the FDIC could experience knowledge and leadership gaps. These gaps may impede the capabilities of the FDIC to achieve its mission, unnecessarily delay decision making, and reduce program management and oversight.[164]

A significant number of FDIC employees responsible for ensuring the safety and soundness of institutions and protecting consumers are also eligible to retire. Approximately 39 percent of RMS staff is eligible to retire within 5 years. Replacing retiring examiners requires lead time, as it generally takes 3 to 4 years for an examiner to complete training. Further, examiners play an important role during financial crises, as they increase bank monitoring and draft required enforcement actions. The FDIC has been over-hiring examiner personnel to address this issue.

Similarly, approximately 34 percent of DCP staff will be eligible to retire within 5 years. The DCP conducts examinations to ensure that banks meet certain requirements for consumer protection, anti-discrimination, and community reinvestment. The FDIC should ensure that there is an effective process for the transfer of the knowledge of seasoned retirement-eligible examiners to junior examiners.

Assessing Potential Retirement Waves in the FDIC's Regional Offices

The FDIC maintains six Regional Offices located throughout the country. Regional Offices include members from all FDIC Divisions, but the largest representation of employees is RMS examination staff. The FDIC faces risks due to staff retirement eligibility rates within each of its Regional Offices.

Based on our analysis, as shown in Table B, we found that FDIC employees in these Regional Offices are eligible to retire within the next 5 years at rates ranging from 33 to 49 percent, and retirement rates for Executives and Managers range from 47 to 76 percent.

[163] GAO, *High-Risk Series: Progress on Many High-Risk Areas, While Substantial Efforts Needed on Others*, GAO-17-317, (February 2017).
[164] Southern California Law Review, *Vacant Offices: Delays In Staffing Top Agency Positions*, (2008).

Table B: Retirement Eligibility Statistics for FDIC Regional Offices

Region	Total Employees	Staff Eligible to Retire in 2025	Executives and Managers Eligible to Retire in 2025
Atlanta	479	35 percent	48 percent
Chicago	538	38 percent	68 percent
Dallas	764	49 percent	70 percent
Kansas City	500	33 percent	76 percent
New York	600	35 percent	47 percent
San Francisco	473	36 percent	61 percent

Source: OIG analysis of FDIC retirement data as of June 1, 2020.

Regional Office personnel are the critical interface between the FDIC and bank management. Regional Office examiners evaluate bank management's controls to maintain safety and soundness, mitigate cybersecurity risks, and minimize harm to consumers. Regional Office personnel also play a significant role during financial crises. For example, the FDIC's resolution and receivership activities are centralized in the Dallas Regional Office where almost half of its staff and 70 percent of Executives and Managers are eligible to retire in the next 5 years. Retirement waves may result in imbalances of senior staff among Regional Offices even where the FDIC increases hiring.

The management of human capital is critical to the FDIC's achieving its mission. The FDIC should continue to manage and align its human capital lifecycle activities – workforce planning, recruitment, hiring, orientation, compensation, engagement, succession planning, and retirement programs – to achieve its mission and goals effectively.

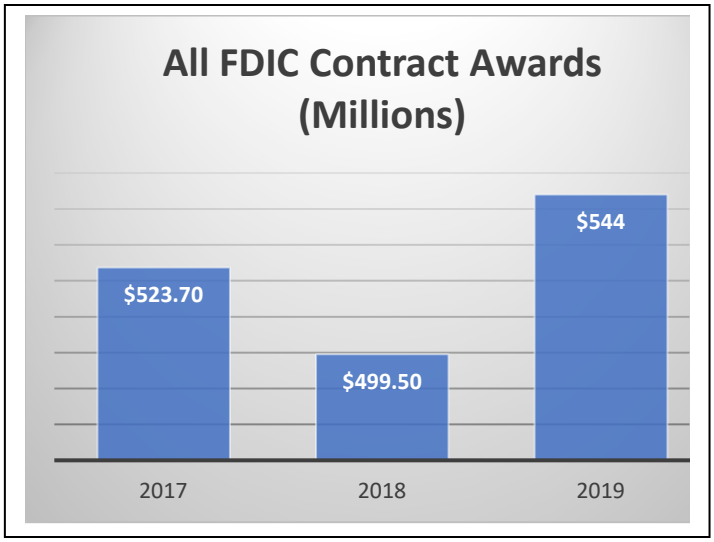
Challenge 9: Overseeing Contracts and Managing Supply Chain Risk

The FDIC is increasingly reliant on contractors for day-to-day support of its mission. Contracting activity escalates during times of crises. The FDIC's budget for 2021 includes an increase of more than $166 million (43.4 percent) for all contractor-provided services. The FDIC should execute a contracting program that ensures effective oversight of the Agency's acquisition of goods and services. In addition, the FDIC should ensure that it adequately manages and mitigates supply chain risks associated with Agency contracts.

The FDIC procures goods and services to augment its internal resources and help the Agency achieve its mission. The FDIC DOA Acquisition Services Branch (ASB) works with Oversight Managers (OM) from FDIC Divisions and Offices to provide oversight of FDIC procurements.

As shown in Figure 3, the FDIC increased contract spending between 2017 and 2019. During this 3-year period, the FDIC awarded larger contracts to fewer companies. Between 2017 and 2019, the FDIC reduced the number of contracts by 30 percent from 737 to 518.

Figure 3: All FDIC Contract Awards 2017-2019



Source: FDIC Division of Administration.

In addition, the FDIC's budget for 2021 includes an increase of more than $166 million (43.4 percent) for contractor-provided services, as reflected in "the establishment of contingency reserves for possible pandemic-related problem bank and/or failure activity" and increased funding for IT modernization. FDIC contracting requirements increase significantly during times of crises due to the FDIC's receivership responsibilities.

Additionally, the FDIC entered into contracts as a result of the pandemic. According to the DOA, as of November 2020, the FDIC spent more than $2 million in pandemic-related contracts, including the purchase of personal protective equipment, specialized cleaning of FDIC Headquarters and Regional Offices, and a management support contract for Covid-19 protocol information.

Strengthening FDIC Contract Oversight

The FDIC may see a further increase in contracting activity as a result of the pandemic. As noted by the GAO in its FDIC financial statement auditor's report included in this Annual Report, the FDIC was found to have a significant internal control deficiency over financial reporting related to contract payment review processes. A significant deficiency is a deficiency, or combination of deficiencies, in internal control that is less severe than a material weakness, yet important enough to merit the attention of those charged with governance. Without adequate contract payment review processes, the FDIC cannot reasonably assure that internal controls over contract payments are operating effectively, thereby increasing the risks that improper payments could occur and misstate the financial statements.

In our OIG evaluation, *Contract Oversight Management* (October 2019), we concluded that the FDIC needs to strengthen its contract oversight management. Specifically, we found that the FDIC was overseeing acquisitions on a contract-by-contract basis rather than on a portfolio basis and did not have an effective contracting management information system to readily gather, analyze, and report portfolio-wide contract information across the Agency. As a result, FDIC Board Members and other senior management officials were not provided with a portfolio-wide view or the ability to analyze historical contracting trends across the portfolio, identify anomalies, and perform ad hoc analyses to identify risk or plan for future acquisitions.

Additionally, 20 percent of the contracts executed between 2013 and 2017 (1,518 of 7,786) did not have contract pricing arrangement information entered into the FDIC's Automated Procurement System. We also found that contract files maintained by OMs were often incomplete, and that OMs were unable to produce the missing contract documentation, such as critical records relating to inspection and acceptance. Without this documentation, the FDIC could incur additional costs to recover or replace lost documentation and could have difficulty enforcing the contract in the event of contractor noncompliance. The FDIC implemented 12 of the 15 recommendations we made to improve the FDIC's contract management, and FDIC officials stated that they are working towards addressing the remaining 3 recommendations, including a new procurement system that will allow for portfolio-wide analysis.

In our ongoing OIG evaluation of the FDIC's Oversight of Blue Canopy, we are assessing whether service contracts between the FDIC and Blue Canopy were for Critical Functions[165] and whether the FDIC performed heightened contract monitoring for Critical Functions. It is important for the FDIC to have a process for identifying Critical Functions during the course of the acquisition planning process. Blue Canopy provides a range of cybersecurity and privacy support services for the FDIC, including continuous monitoring, vulnerability management, internal control reviews, and privacy assessments. These services are critical to ensuring the security and protection of the FDIC's IT infrastructure and data. A breach or disruption in these services could affect the security, confidentiality, integrity, and availability of the information and data at the FDIC.

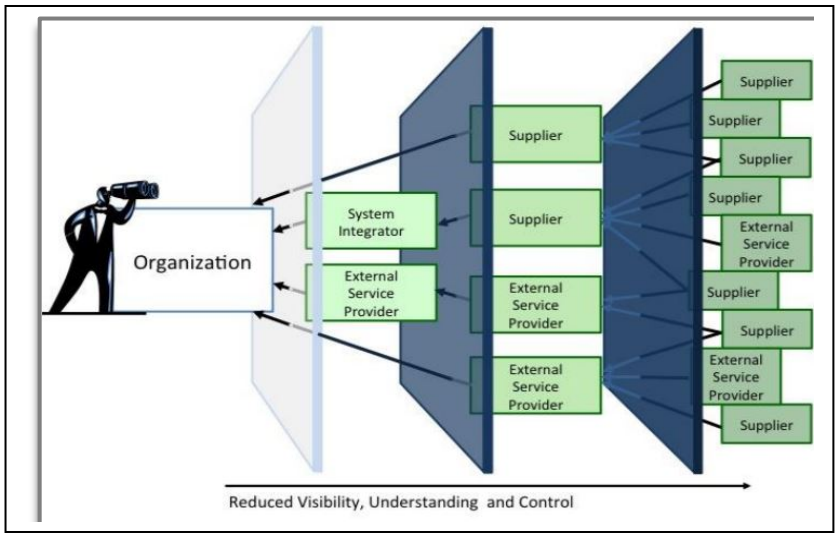
It is also important for the FDIC to have heightened contract monitoring activities for Critical Functions. Without these practices in place, the FDIC may not retain oversight resources at a sufficient level of capacity and capability, including an adequate number of its employees with the appropriate training and experience. In addition, the FDIC may not conduct proper oversight to understand the Agency's requirements, formulate alternatives, manage work products, and monitor contractors used to support the Federal workforce.

[165] A critical function is a function that is necessary to the Agency being able to effectively perform and maintain control of its mission and operations. Typically, critical functions are recurring and long-term in duration. *See* OMB Policy Letter 11-01, *Performance of Inherently Governmental and Critical Functions*, 76 Fed. Reg. 56227 (September 11, 2011).

Assessing Supply Chain Risk

When an agency contracts for goods and services that will be introduced into its environment, the agency might encounter risks related to product and service supply chains.[166] As shown in Figure 4, an organization may have reduced visibility, understanding, and control of relationships with vendors who rely on second- and third-tier suppliers and service providers.

Figure 4: Supply Chain Risk



Source: NIST Publication 800-161.

Risks are realized when the supply chain exploits existing vulnerabilities, though it may take years for such exploitation to occur or for an agency to discover the exploitation. The GAO noted that key supply chain threats include, for example, hardware and software installations that allow hackers to take control and counterfeit hardware and software that threaten systems integrity and reliability.[167] Further, supply chain production and service risks can disrupt the supply of critical IT products and allow malicious or unqualified service providers to disrupt operations.[168]

According to NIST guidance, management of supply chain risk requires "ensuring the integrity, security, quality, and resilience of the supply chain and its products and services."[169] NIST guidance describes supply chain risk as including an "organization's decreased visibility into, and understanding of how the technology that they acquire is developed, integrated, and deployed." NIST guidance further advises organizations to take a holistic, enterprise-wide approach to managing supply chain risks.[170] The OMB required agencies to implement information and communications technology supply chain risk management principles.[171]

On July 14, 2020, the Department of Defense, General Services Administration, and National Aeronautics and Space Administration issued a joint Interim Rule[172] addressing

---

[166] NIST, *Cyber Supply Chain Risk Management,* (May 24, 2016).
[167] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T, (July 12, 2018).
[168] GAO, *Information Security: Supply Chain Risks Affecting Federal Agencies*, GAO-18-667T, (July 12, 2018).
[169] NIST, *Cyber Supply Chain Risk Management*, (May 24, 2016).
[170] NIST Special Publication 800-161, *Supply Chain Risk Management for Federal Information Systems and Organizations*, (April 2015).
[171] OMB, *Circular A-130, Managing Information as a Strategic Resource*, (July 2016).
[172] The Office of the Federal Register's, *Guide to the Rulemaking Process,* defines an Interim Rule as a final rule that is published without first publishing a proposed rule for notice and comment.

the Federal Government's procurement supply chain risks for telecommunication and video surveillance services or equipment.[173] Effective August 13, 2020, the Interim Rule prohibits Federal Executive Agencies that follow the Federal Acquisition Regulations from contracting with certain Chinese companies, including Huawei and ZTE.[174]

As mentioned previously, in December 2020, it was reported that Federal Government agency networks were compromised by a software update from the IT management services company SolarWinds.[175] By exploiting supply chain vulnerabilities, nation-state actors inserted malicious code into a SolarWinds software update, which gave hackers access to Government systems.[176] The Cybersecurity and Infrastructure Security Agency (CISA) issued an Emergency Directive to Federal agencies "to review their networks for indicators of compromise and disconnect or power down their SolarWinds Orion products immediately."[177] CISA stated that the threat of the SolarWinds compromise poses a great risk to the Federal Government.[178]

The FDIC uses a SolarWinds product. Following the issuance of the Emergency Directive, FDIC officials represented that they had disconnected the FDIC SolarWinds product and that they were in the process of conducting an internal review.

Also in December 2020, the National Security Agency (NSA) issued a Cybersecurity Advisory that nation state actors exploited a vulnerability in VMware products that allows attackers to forge security credentials and gain access to protected data.[179] The Cybersecurity Advisory recommended application of a vendor-issued patch. The FDIC uses a VMware product, and FDIC officials represented that they took action to apply the patch and reduce the risk of exploitation for the FDIC VMware product.

In November 2019, the FDIC initiated the Supply Chain Risk Management Implementation Project (SCRM Project) to build a supply chain risk-aware culture and establish an SCRM framework and governance structure. The SCRM Project is

---

[173] Federal Acquisition Regulation: *Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment*, 85 Fed. Reg. 42665 (July 14, 2020). The interim rule implements section 889(a)(1)(B) of the John S. McCain National Defense Authorization Act (NDAA) for Fiscal Year 2019 (Pub. L. 115–232).

[174] Federal Acquisition Regulation*: Prohibition on Contracting with Entities Using Certain Telecommunications and Video Surveillance Services or Equipment*, 85 Fed. Reg. 42665 (July 14, 2020). The statute covers certain telecommunications equipment and services produced or provided by Huawei Technologies Company or ZTE Corporation (or any subsidiary or affiliate of those entities) and certain video surveillance products or telecommunications equipment and services produced or provided by Hytera Communications Corporation, Hangzhou Hikvision Digital Technology Company, or Dahua Technology Company (or any subsidiary or affiliate of those entities).

[175] The Washington Post, *Russian Government Hackers are Behind a Broad Espionage Campaign That Has Compromised U.S. Agencies Including Treasury and Commerce,* (December 14, 2020).

[176] The New York Times*, Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit*, (December 14, 2020).

[177] CISA*, CISA Issues Emergency Directive To Mitigate The Compromise Of SolarWinds Orion Network Management Products,* (December 14, 2020).

[178] CISA Cyber Activity Alert, *Advanced Persistent Threat Compromise of Government Agencies, Critical Infrastructure, and Private Sector Organizations*, (December 17, 2020); The New York Times*, Scope of Russian Hack Becomes Clear: Multiple U.S. Agencies Were Hit*, (December 14, 2020). Politico, *How Suspected Russian Hackers Outed Their Massive Cyberattack*, (December 16, 2020).

[179] NSA Cybersecurity Advisory, *Russian State-Sponsored Malicious Cyber Actors Exploit Known Vulnerability in Virtual Workspaces*, (December 7, 2020).

governed by a steering committee,[180] coordinated by a project manager, and executed by a working group. The SCRM project manager uses a project plan to manage SCRM tasks. According to the FDIC, in 2020, the SCRM officials issued a Procurement Administrative Bulletin requiring SCRM-related provisions and clauses in all future FDIC solicitations and awards, as well as any contract extensions or updates of existing contracts. SCRM officials also indicated that they had a draft FDIC directive on supply chain management that is currently under review. We will continue monitoring and assessing the FDIC's efforts in this regard.

The FDIC should ensure effective oversight of its increasing contractor portfolio. Contract oversight strengthens prudent management of FDIC resources and ensures that the FDIC receives expected goods and services. FDIC contracting should also take into consideration supply chain risk in order to keep FDIC information, assets, and personnel safe and secure.

Challenge 10: Enhancing Rulemaking at the FDIC

FDIC rulemaking places requirements upon supervised banks, and such impositions often affect individual deposit holders as well. The FDIC should have a transparent rulemaking process that balances the need for safety and soundness regulation and the burden on financial institutions' regulatory compliance. It is also important to ensure that rulemakings do not promote regulatory capture by serving the interest of banks at the expense of the public. A foundational component of rulemaking is the FDIC's access to reliable information to measure a regulation's costs and benefits.

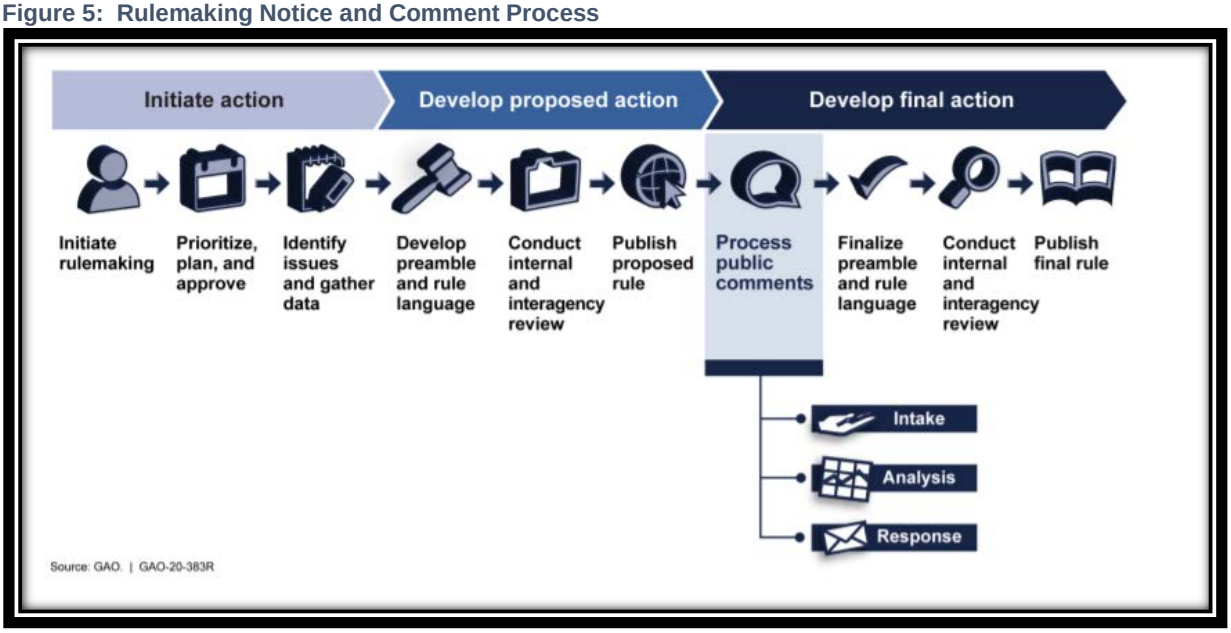
The GAO estimates that "Federal agencies publish on average 3,700 proposed rules yearly."[181] The cost of compliance with regulations impacts financial institutions. According to the International Banker, annual bank compliance cost is estimated to be $270 billion.[182] Further, a study by the Federal Reserve Bank of St. Louis found that regulatory compliance costs as a percentage of overall non-interest expense for small banks are nearly twice those for larger banks.[183]

[180] Steering Committee membership includes Assistant General Counsel, Legal Division, Corporate and Legal Operations Section; Associate Director, Division of Resolutions and Receiverships, Receivership Operations Branch; Deputy Director, CIO Acquisition Strategy and Innovation Branch; Chief Risk Officer and Deputy Director, Division of Finance, Risk Management and Internal Controls Branch; Deputy Director, Division of Administration, Acquisition Services Branch; and Special Advisor to the Chief Operating Officer.
[181] Statement of Seto J. Bagdoyan, Director of Audits, Forensic Audits and Investigative Service, before the Permanent Subcommittee on Investigations and the Subcommittee on Regulatory Affairs and Federal Management, Committee on Homeland Security and Governmental Affairs, United States Senate, *Federal Rulemaking: Selected Agencies Should Clearly Communicate Public Comment Posting Practices Associated with Identity Information*, GAO-20-105T, (October 24, 2019).
[182] International Banker, *Cost of Compliance*, (November 7, 2018).
[183] Federal Reserve Bank of St. Louis, *Compliance Costs, Economies of Scale and Compliance Performance, Evidence from a Survey of Community Banks*, (April 2018).

Improving the FDIC's Rulemaking Process

Federal agencies must follow the requirements of the Administrative Procedure Act (APA), which governs Federal rulemaking and outlines processes that Federal agencies must complete when promulgating regulations. Agencies have their own rulemaking policies and practices for implementing the APA procedures.[184] Figure 5 provides an overview of the process agencies use for rulemaking notice and comments.[185]

Figure 5: Rulemaking Notice and Comment Process



The Banking Act of 1933 provided the FDIC with the authority to issue rules to fulfill the Agency's mission. Agencies, like the FDIC, develop rules to achieve agency goals and objectives, and implement Federal statutes. The FDIC's resource and process guide entitled, *Development of FDIC Rules and Statements of Policy* (July 2018) states that the "rulemaking process is most effective and efficient when rulemaking analytical requirements are addressed beginning in the early phases of a rule's development and revisited as necessary while development progresses."

Improving Cost Benefit Analysis. Measuring the costs and benefits of regulations is an important rulemaking function. According to the *FDIC's Statement of Policy on the Development and Review of Regulations and Policies*, the FDIC uses available information to evaluate the costs and benefits of reasonable and potential regulations or statements of policy. Quantifying both the costs and benefits of significant financial regulations is challenging, and it often may be imprecise and unreliable.[186] For example, the process does not take into account environmental impacts, and large industries or companies with resources may easily produce cost data while agencies may have

[184] GAO, *Federal Rulemaking: Information on Selected Agencies' Management of Public Comments*, GAO-20-383R, (April 16, 2020).
[185] GAO, *Federal Rulemaking: Information on Selected Agencies' Management of Public Comments*, GAO-20-383R, (April 16, 2020).
[186] Yale Law Journal Forum, *Cost-Benefit Analysis of Financial Regulation: A Reply*, (January 22, 2015).

difficulty quantifying broad societal benefits.[187] Performing such analysis can be difficult, because it involves theory, modeling, statistical analysis, and other tools to predict future outcomes based upon certain assumptions.[188] To illustrate, it may be difficult to estimate the cost of a financial crisis and the benefits of regulations aimed to mitigate the risks associated with a crisis.[189]

In our OIG evaluation, *Cost Benefit Analysis Process for Rulemaking* (February 2020), we found that the FDIC's rulemaking processes were inconsistent with five identified best practices. The FDIC:

- Had not established and documented a process to determine when and how to perform cost benefit analyses;
- Did not leverage the expertise of its economists during initial rule development;
- Did not require the FDIC Chief Economist to concur on the cost benefit analyses performed;
- Was not transparent in its disclosure of cost benefit analyses to the public; and
- Did not perform cost benefit analyses after final rule issuance.

As a result, the FDIC's rulemaking process resulted in inconsistent practices for conducting cost benefit analyses. Based on our review of rules finalized by the FDIC from January 2016 to December 2018, we found that the FDIC performed cost benefit analyses on 15 of 40 final rules (37 percent) published in the Federal Register. The FDIC did not publish its rationale as to why 25 rules issued by the FDIC did not warrant cost benefit analysis. Further, we found that the FDIC performed an in-depth cost benefit analysis on only 4 of 40 final rules (10 percent) published in the Federal Register. In addition, the FDIC's depth of analysis for a particular rule did not always align with the rule's substance. Without thorough and consistent cost benefit analyses, the FDIC could implement or enforce poorly conceived or overly burdensome rules. The FDIC has provided a timeline to implement corrective actions to address our recommendations.

Conducting Retrospective Review of Regulations. Best practices support that agencies should establish and document a process to perform retrospective analyses of their issued rules or, at a minimum, perform a regulatory risk assessment to identify those rules or rule provisions that are at higher risk of being outdated, duplicative, or unduly burdensome.[190] Risk assessment may allow agencies to identify those rules or rule provisions that should be subject to a more thorough retrospective cost benefit analysis. These analyses can inform policy-maker judgments about whether to modify, expand, streamline, or repeal such regulations. Retrospective cost benefit analysis can also provide valuable insight on the strengths and weaknesses of the agency's rulemaking, by facilitating a comparative analysis of expected effects to actual effects, which can be used to enhance the agency's analytic capability.

---

[187] Center for American Progress, *Reckoning With Conservatives' Bad Faith Cost-Benefit Analysis*, (August 14, 2020).
[188] Congressional Research Service, *Cost-Benefit Analysis and Financial Regulator Rulemaking*, (April 12, 2017).
[189] The University of Chicago Journal of Legal Studies, *Challenges for Cost-Benefit Analysis of Financial Regulation*, (June 2014).
[190] According to Executive Order 13579 and OMB Memorandum M-11-28, independent regulatory agencies are encouraged to engage in a retrospective analysis of the costs and benefits (both quantitative and qualitative) of regulations chosen for review.

In our evaluation, *Cost Benefit Analysis Process for Rulemaking* (February 2020), we found that the FDIC did not perform cost benefit analyses after issuance of the rule. Without performing cost benefit analyses of existing rules or establishing a formal process to proactively review each final rule, the FDIC may not identify duplicative, outdated, or overly burdensome rules in a timely manner. In addition, the FDIC may not ensure that its rules are effective and continue to achieve their intended objectives and outcomes.

FDIC rulemaking should be transparent and grounded in analysis demonstrating that a rule's benefits outweigh its costs. By obtaining concrete, valid, and reliable data, the FDIC can analyze the costs and benefits of regulations before implementing a rule. Further, retrospective analysis of the costs and benefits of issued rules would allow the FDIC to determine whether the rule should be modified or repealed.