Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation

February 2023

Federal Deposit Insurance Corporation
Office of Inspector General

NOTICE

Pursuant to Pub. L. 117-263, section 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to comments@fdicoig.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information.

Date: February 16, 2023

Memorandum To: Board of Directors

/Signed/
From: Tyler Smith
Acting 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). This document summarizes the most serious challenges facing the FDIC and briefly assesses 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. In several instances, we discuss topic areas where the OIG has previously conducted work to evaluate, audit, and review the FDIC's progress in these Challenge areas.

We identified nine Top Challenges facing the FDIC. These Challenges include all aspects of the Challenges that we reported last year, with important updates. Among these updates are the need for supervisory attention and crises planning to include executing its resolution processes, examining banks' compliance with U.S.-imposed sanctions, and assessing digital asset risk. The Challenges identify risks to FDIC mission-critical activities and to FDIC internal programs and processes that support mission execution.

The FDIC's Top Challenges include:

1. Preparing for Crises in the Banking Sector
2. Mitigating Cybersecurity Risks at Banks and Third Parties
3. Supervising Risks Posed by Digital Assets
4. Fostering Financial Inclusion for Underserved Communities
5. Fortifying IT Security at the FDIC
6. Managing Changes in the FDIC Workforce
7. Improving the FDIC's Collection, Analysis, and Use of Data
8. Strengthening FDIC Contracting and Supply Chain Management
9. Implementing Effective Governance at the FDIC

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. This researched and deliberative analysis guides our work, and we believe it is 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.

Executive Summary

The FDIC plays a unique role in support of the U.S. financial system. The FDIC insures nearly $10 trillion in deposits at more than 4,700 banks, supervises over 3,200 banks, and oversees the $125 billion Deposit Insurance Fund (DIF) that protects bank depositor accounts and resolves failing banks. The readiness of the FDIC to execute all facets of its mission promotes confidence and stability in the Nation's financial system.

Currently, banks are facing a rising interest rate environment while the U.S. economy faces inflationary pressure and continued uncertainties remain resulting from Russia's invasion of Ukraine. Banks have also adopted new technologies and third-party partnerships to engage customers at a time of increasing cyber security breaches. Banks are also entering into markets for digital assets, which may increase money laundering and terrorist financing risks. The FDIC's operating environment is also changing. The FDIC moved to a hybrid working environment and faces increased retirements and resignations among FDIC personnel.

In light of these circumstances, this document summarizes the most serious challenges facing the FDIC and briefly assesses the Agency's progress to address them, pursuant to the Reports Consolidation Act of 2000 and Office of Management and Budget Circular A-136 (revised August 27, 2020). This 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. 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.

We identified nine Top Challenges facing the FDIC that could impact its capabilities to promote public confidence and financial stability:

Preparing for Crises in the Banking Sector. The FDIC has a unique mission to administer the DIF and insure Americans' bank deposits against losses during crises. The FDIC's effective maintenance of the DIF, supervision of banks, and resolution of failed banks provides financial stability to the United States. The FDIC faces crises readiness challenges to fully develop its plans to respond to an unfolding crisis, including exercising the orderly liquidation of systemically important entities. Further, FDIC readiness and supervisory activities should take into account climate-related risks. FDIC supervisory processes should also be agile to respond to evolving risks such as fraud in crises-related Government-guaranteed loan programs and the evasion of US-imposed economic and trade sanctions.

Mitigating Cybersecurity Risks at Banks and Third Parties. Cybersecurity has been identified as the most significant threat to the banking sector and the critical infrastructure of the United States. The FDIC faces challenges to ensure that examiners have the skillsets and knowledge to conduct information technology examinations that adequately identify and mitigate cybersecurity risks at banks and their third-party service providers (TSP). Further, the FDIC should ensure that it has effective processes for the intake of banks' cybersecurity incident reports and uses these reports to mitigate identified risks, identify trends and patterns of nefarious activity, and adjust supervisory processes. Mitigating cybersecurity risk is critical, as a cyber incident at one bank or TSP has the potential to cause contagion within the financial sector.

Supervising Risks Posed by Digital Assets. About 52 million Americans have invested in digital assets and 136 FDIC-insured banks have ongoing or planned digital asset activities. The FDIC should work with other regulators to provided clarity regarding the regulation of digital

assets. The FDIC should also have examiners with appropriate skillsets and examination processes to assess the safety and soundness of banks' digital asset activities and identify consumer risks. Further, the FDIC should ensure that its examinations, policies, and procedures address consumer risks regarding digital assets, including the relationship of deposit insurance and digital assets.

Fostering Financial Inclusion for Underserved Communities. Federal statute mandates that the FDIC study the unbanked market in the United States and identify the primary issues that prevent unbanked individuals from establishing conventional accounts in financial institutions. Converting the information gleaned from the study of unbanked individuals into effective actions that banks can take to increase access to the financial system for unbanked individuals is a challenging endeavor for the FDIC. Further, the FDIC should also ensure that its examiners have the skills, capabilities, and procedures to assess the effect of banks' use of artificial intelligence (AI) in decision making. AI can be beneficial by increasing the speed and reducing the cost of bank operations, but it can also result in biases against individuals when the algorithms or data used for these decisions are flawed.

Fortifying IT Security at the FDIC. The FDIC is custodian of about 1.8 petabytes of sensitive and Personally Identifiable Information (PII) relating to failed banks and more than 4,700 insured banks. The FDIC continues to face challenges to ensure that it has strong information security processes to guard against persistent and increasing cyber threats against Federal agencies. Security control weaknesses of FDIC systems limit the effectiveness of FDIC controls, which places the confidentiality, integrity, and availability of FDIC systems and data at risk. The FDIC should have robust personnel security and suitability program and privacy controls to safeguard IT access to sensitive information and guard against insider threats.

Managing Changes in the FDIC Workforce. A total of 21 percent of the FDIC workforce was eligible to retire in 2022, and that figure climbs to 38 percent within 5 years (2027). These retirements may have a significant impact on key Divisions involved in Crises Readiness efforts and for subject matter experts in areas such as consumer compliance and information technology. At the same time, the FDIC is experiencing increased resignations of its examiners-in-training. Absent effective human capital management, the FDIC may lose valuable knowledge and leadership skill sets upon the departure of experienced examiners, managers, and executives. Meeting these challenges is especially important as the FDIC shifts its operations to a hybrid environment.

Improving the FDIC's Collection, Analysis, and Use of Data. Data and information can enhance the FDIC's and its supervised banks' capabilities to mitigate threats to the U.S. financial system. The FDIC faces challenges in receiving and using reliable information. Specifically, the FDIC should establish processes to acquire, analyze, and disseminate threat information from Government partners, databases, and repositories. Such information informs senior FDIC officials and decision-makers, FDIC examiners and Regional personnel, its supervisory program officials, and banks. Further, the FDIC should improve the reliability of its internal data to ensure that the FDIC Board and senior management can confidently use the data to assess program effectiveness.

Strengthening FDIC Contracting and Supply Chain Management. The FDIC awards nearly $600 million in contracts every year. Over a 5-year period, the FDIC awarded more than 2,600 contracts valued at $2.85 billion. The FDIC faces challenges to establish an effective contract management program that ensures the FDIC receives goods and services according to contract terms, price, and timeframes. An effective FDIC procurement program is important because the

FDIC relies on contractor services for day-to-day activities and especially during crises. The FDIC should also have programs in place to mitigate security risks associated with the supply chains for contracted goods and services. Weaknesses in contractor-provided software to Government agencies have exposed examples of these supply chain risks. Further, the FDIC should have whistleblower processes and provisions within FDIC contracts to protect contractor personnel who report allegations of contractor violations and gross mismanagement.

Implementing Effective Governance at the FDIC. Effective governance allows FDIC Board members and senior FDIC officials to proactively manage risk, formulate regulatory policy, and provide clear guidance to banks and FDIC Regional Offices. Through these processes, the FDIC can allocate resources, prioritize and improve the flow of risk information to decision makers, and work toward achieving the FDIC's mission. The FDIC should ensure that risks to the FDIC are identified and monitored through an effective Enterprise Risk Management Program. The FDIC should also ensure that OIG-identified program weaknesses are promptly resolved and remediated. FDIC program performance should be measured using outcome measures to assess whether the FDIC is meeting a program's strategic objectives. The FDIC should also clarify its implementation of Executive Branch best practices, ensure the validity of its rulemaking process, and promulgate rules based on rigorous cost benefit analyses.

The FDIC has taken certain concrete and measurable steps to address some of these Challenges, as noted in this Challenges document. 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.

Preparing for Crises in the Banking Sector

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Executing orderly liquidation processes;
- Enhancing readiness for crises;
- Addressing climate risks to banks;
- Mitigating pandemic loan fraud; and
- Ensuring banks' compliance with U.S. sanctions.

The OIG has identified Preparing for Crises as a Top Challenge for the FDIC since 2018.

The Board of Governors of the Federal Reserve (Federal Reserve Board) stated that U.S. financial stability may be affected by sudden adverse events.[1] These events may include cyber attacks, climate change risk, and global instability.[2] The U.S. financial system also faces risks arising internationally from outside the United States through "a contagious spread of a financial crisis" across regions and countries.[3] Financial instability could result in failures for banks, broker-dealers, financial market utilities, insurance companies, and other systemically important organizations that could require the FDIC to exercise its expansive resolution authorities.

In addition, according to the Financial Stability Oversight Council's Report on Climate-Related Financial Risk 2021 (FSOC Climate Report) (October 2021), climate change continues to grow as an emerging threat to the financial stability of the United States. The National Oceanic and Atmospheric Administration reported 18 weather and climate-related disaster events in 2022 with losses exceeding $1 billion across the United States. The Organization for Economic Co-operation and Development (OECD) also noted that the transition to low-carbon economies may result in financing risks for stranded or obsolete assets and production processes that do not support renewable energy.[4] The 60 largest banks financed $4.6 trillion in loans to fossil fuel companies between 2016 and 2021.[5]

The banking sector also faces risks related to the Government's response to the pandemic crisis. In 2020 and 2021, the Coronavirus Aid, Relief, and Economic Security Act (CARES Act) and the American Rescue Plan were enacted, and these laws provided funds for the Paycheck Protection Program (PPP) in the amount of $814 billion. The PPP has been administered through the Nation's banks. It is estimated that fraud in the PPP could be as high as $117.3 billion, and banks may suffer losses as a result of fraudulent loans.[6]

In addition, the Department of the Treasury's Office of Foreign Assets Control (OFAC) administers economic and trade sanctions that prohibit domestic banks from conducting transactions with a number of entities sanctioned by the United States. For example, the U.S. recently imposed additional sanctions against Russia in response to a crisis presented by the invasion of Ukraine. If banks do not have sufficient compliance programs to adhere to the U.S. sanctions, they may face increased legal, compliance, operational, and reputational risks, and significant enforcement actions.

Executing Orderly Liquidation Processes

The FDIC is the primary Federal agency responsible for the resolution of insured depository institutions. The FDIC's authority stems from the Federal Deposit Insurance Act (FDI Act), which allows the FDIC to pay insured deposits and become a receiver of failed banks. The FDIC's resolution

authority under the FDI Act, however, does not apply to certain financial institutions, such as investment banks, insurance companies, broker-dealers, and other systemically important financial institutions.[7] As a result, during the financial crisis of 2008-2011, several large financial firms—such as Lehman Brothers, Bear Stearns, and AIG—were not eligible for FDIC receiverships.[8] In response, Title II of the Dodd-Frank Wall Street Reform and Consumer Protection Act of 2010 (Dodd-Frank Act) was enacted and designed to address this gap, and granted Orderly Liquidation Authority (OLA) to the FDIC.

OLA presents unique challenges for the FDIC because this authority has not been invoked, and the FDIC has limited information and experience with financial market utilities, insurance companies, and broker-dealers that may require OLA resolutions. The FDIC should be ready to swiftly execute its OLA in an efficient manner. In December 2013, the FDIC published a strategy to execute an orderly liquidation.[9] The strategy includes a number of steps, including: (i) coordination among the FDIC, the Department of the Treasury, and other banking regulators; (ii) hiring qualified executives to run the holding company; (iii) communicating with staff, shareholders, and the public regarding the status of the receivership; and (iv) contracting and coordination within FDIC Divisions and Offices.

The FDIC should clearly define policies, procedures, roles, and responsibilities to ensure efficient implementation of its OLA authorities. Absent such clarity, the resolution may not effectively address an entity's failure, thus impeding mitigation of systemic risk throughout the financial system. We have work ongoing to determine if the FDIC has established key elements to execute its OLA, including comprehensive policies and processes, necessary resources and skill sets, and integration with the Agency's crisis readiness and response planning efforts.[10]

Current areas of focus for resolution planning under OLA include domestic bank holding companies designated as "global systemically important banks" (GSIB),[11] U.S. holding companies of foreign-based GSIBs,[12] and systemically important financial market utilities (FMU) designated by FSOC.[13] The FDIC, however, does not supervise or examine FMUs and, as a result, has limited expertise or familiarity with their operations. Similarly, the FDIC does not have examination or supervisory authority over broker-dealers and therefore has limited knowledge of their operations.

Enhancing Readiness for Crises

In April 2020, we issued an OIG evaluation report, The FDIC's Readiness for Crises, regarding the FDIC's execution of FDI Act resolutions, which found that the FDIC did not have documented Agency policy and procedures for crisis readiness planning and did not have an Agency-wide all hazards readiness plan nor Agency-wide hazard-specific readiness plans. The FDIC needed to fully establish seven elements of crisis readiness to be prepared to respond to any type of crisis that may impact the banking system: (1) policies and procedures; (2) plans; (3) training; (4) exercises; (5) lessons learned; (6) maintenance; and (7) assessment and reporting. The FDIC has addressed the report recommendations.

Subsequent to our report, the Council of Inspectors General on Financial Oversight issued its Guidance in Preparing for and Managing Crises (June 2022).[14] This Guidance identified critical activities for pre-crisis planning and crisis management that FSOC and member agencies can use to evaluate existing efforts and coordinate and plan for future crises. The Guidance includes three activity categories:

- **Collaboration and Pre-Crisis Planning**. A proactive crisis readiness effort involves working collaboratively to coordinate crisis

readiness efforts across Federal, state, and international agencies by: (1) identifying risks and conducting scenario analyses; and (2) developing plans ahead of time that outline how an agency will respond to crises.

- **Crisis Readiness Plan Elements**. Crisis readiness plans create an overarching framework for crisis management to include strategic decision-making, communication, and coordination.

- **Crisis Management.** The key elements to managing a crisis effectively include clear leadership response, coordination, communication, resource assessments, supervisory activities, and implementation of response or rescue programs.

The FDIC should continuously assess its own preparedness efforts and make changes to address any gaps in its readiness.

Addressing Climate Risks to Banks

The FDIC should be prepared to address banks' climate-related risks, including how these risks may affect FDIC bank examinations and supervision. For example, the FDIC may need to increase the information it collects from banks, reassess bank stress testing, and review banks' concentrations in industry financing of fossil fuels. The FDIC also may need to revise its supervisory strategies and examination procedures to address climate risks.

On May 20, 2021, the President issued Executive Order 14030, Climate-Related Financial Risk, which required that FSOC, including the FDIC:

- Assess, in a detailed and comprehensive manner, the climate-related financial risk, including both physical and transition risks, to the financial stability of the Federal Government and the stability of the U.S. financial system;
- Facilitate the sharing of climate-related financial risk data and information among FSOC member agencies and other executive departments and agencies as appropriate; and
- Issue a report to the President within 180 days of the date of the order on any efforts by FSOC member agencies to integrate consideration of climate-related financial risk in their policies and programs.

The FSOC Climate Report issued 30 recommendations to its members related to four topic areas to strengthen the financial system and lessen the vulnerabilities to climate-related shocks:

- Building capacity and expanding efforts to address climate-related financial risks.
- Filling climate-related data and methodology gaps.
- Enhancing public climate-related disclosures.
- Assessing and mitigating climate-related risks that could threaten the stability of the financial system.

The FSOC Climate Report also noted that a climate event may "disproportionately affect financially vulnerable populations potentially including lower-income communities, communities of color, Native American communities, and other disadvantaged or underserved communities." For example, a study of weather-related climate issues conducted by the FDIC Division of Insurance and Research, Severe Weather Events and Local Economic and Banking Conditions (June 2022), concluded that climate change events affect areas

differently based on the health and resiliency of the economy preceding the event.

The FDIC 2022 Annual Performance Plan noted that to "address the risks to the safety and soundness of financial institutions and the stability of the financial system, the FDIC will establish an interdivisional working group to assess the enumerated risks and provide advice to staff developing interagency guidance. The FDIC will also join the international Network of Central Banks and Supervisors for Greening the Financial System."

In April 2022, the FDIC issued a Notice of Proposed Policy Statement on a high-level framework for banks' management of climate-related financial risk. As of the writing of this Top Challenges Report, the FDIC continues to review the comments received on this high-level framework. However, to date, the FDIC has not issued guidance regarding climate change to its examiners or to the banks.

In November 2022, the FDIC also added climate-related financial risk to its Risk Inventory as part of the FDIC's Enterprise Risk Management (ERM) program. The purpose of ERM is to capture risk areas and guide FDIC resources and decision-making to address such risks. On November 15, 2022, the then-Acting Chairman of the FDIC stated that the Agency "is still in the beginning stages of [its] work on climate-related financial risks."[15]

In order to address the FSOC Climate Report recommendations, the FDIC would need a coordinated effort among its Divisions and Offices, other regulators, and international organizations. In so doing, the FDIC would need to continue to gather data related to climate change risks to banks and establish processes to define, measure, monitor, assess, and report on these risks. Further, based upon identified risks, the FDIC would need to provide guidance to banks and examiners for risk mitigation, update existing policies and processes, and formulate new regulations as needed.

We will continue to monitor FDIC efforts in this area, and we are participating in the efforts of the Council of Inspectors General on Financial Oversight to assess FSOC's efforts to address the requirements of Executive Order 14030.

Mitigating Pandemic Loan Fraud

In response to the pandemic, the CARES Act established the PPP, which was intended to provide financial relief to workers, small businesses, and individuals most in need during the pandemic. PPP loans were guaranteed by the Small Business Administration (SBA), if lenders complied with program requirements.

More than 2,600 FDIC-supervised financial institutions originated over 3 million PPP loans, totaling approximately $267 billion. Government-guaranteed loans also introduce other risks such as Operational, Compliance, Liquidity, Reputation, and Strategic Risks.[16] For example, when financial institutions fail to materially comply with Government-guaranteed loan program requirements in the areas of loan underwriting, closing, and servicing, those Federal agencies guaranteeing the loans can be released from their obligations. The originating bank is therefore responsible for the entire loan amount.

It is estimated that fraudulent loans in the PPP may amount to $117.3 billion. For example, the SBA OIG's Inspection of SBA's Implementation of the Paycheck Protection Program reported that nearly 55,000 PPP loans worth about $7 billion went to potentially ineligible businesses or fraudulent recipients and 1.9 million loans were disbursed where the loan participants did not submit loan forgiveness applications—a key fraud indicator. Further, as of October 2022, the Government has brought charges against 1,616 defendants

related to 1,050 criminal cases involving more than $1.2 billion in pandemic relief program funds.[17] We have an evaluation ongoing to assess the FDIC's examination of Government-guaranteed loans.

Ensuring Banks' Compliance with U.S. Sanctions

The U.S. imposes sanctions on countries and organizations that threaten the U.S. economy, foreign policy, and national security. For example, in response to Russia's invasion of Ukraine, the United States imposed sanctions on organizations and entities related to the Russian government.

OFAC regulations require that financial institutions block or reject transactions subject to sanctions, thereby limiting sanctioned parties' access to funding. In addition, banks must notify OFAC of blocked or rejected transactions within 10 days of their occurrence and report all blocked property to OFAC annually by September 30. In addition, banks are required to file Suspicious Activity Reports with the Financial Crimes Enforcement Network (FinCEN) for potential evasion of the sanctions. If a bank's compliance program is inadequate, it faces increased legal, compliance, operational, and reputational risks and significant enforcement action.

In February 2022, the U.S. announced sanctions against major Russian banks and specific Russian individuals.[18] On March 7, 2022, FinCEN alerted banks to be vigilant against attempts to evade sanctions.[19] FinCEN provided a list of red flag indicators of evasion of sanctions, such as the use of third parties to shield the identity of sanctioned persons, the use of shell companies for wire transfers, and non-routine foreign exchange transactions.

FDIC examinations should ensure that banks uphold and comply with the requirements of the sanctions. According to FDIC examination guidance, banks "should establish and maintain effective OFAC programs and screening capabilities in order to facilitate safe and sound banking practices." The guidance continues that "examination procedures should focus on evaluating the adequacy of an institution's overall OFAC compliance program and procedures, including the systems and controls in place to reasonably assure accounts and transactions are blocked and rejected." We have work planned to assess the effectiveness of the FDIC's examination of banks' sanctions compliance programs.

The FDIC should be prepared to address any sort of crisis affecting the U.S. banking sector— whether it is a financial crisis or one due to climate change, a pandemic, or foreign war. To ensure effective execution of resolutions, the FDIC should ensure that it has clear policies, defined roles and responsibilities, effective organizational processes, trained individuals, and ample resources. The FDIC also should ensure that it makes necessary supervisory adjustments to policy and examinations to address emerging risks such as climate change. Further, FDIC examinations should review for Government-guaranteed loan risks, including risks related to the PPP. FDIC examinations also should assess banks' compliance programs to block and reject financial transactions by individuals and entities subject to U.S. sanctions.

Mitigating Cybersecurity Risk at Banks and Third Parties

Key Areas of Concern

The primary areas of concern for this Challenge area are:

- Ensuring FDIC examinations address cybersecurity risks at banks;
- Examining for third-party risk; and
- Recording and assessing banks' cybersecurity incidents.

The OIG has identified Cybersecurity in the banking sector as a Top Challenge for the FDIC since 2018.

The FSOC 2022 Annual Report recognized that a cybersecurity incident could threaten U.S. financial stability. FSOC stated that the "financial sector is vulnerable to malicious cyber incidents, including ransomware, denial-of-service attacks, data breaches, and non-malicious cyber incidents." FSOC noted that millions of Americans could be affected by cybersecurity incidents that result in billions of dollars in financial losses.

The financial industry suffered the largest number of data breaches in 2021 when compared to 20 other industries, according to Verizon's 2022 Data Breach Incident Report.[20] In November 2022, FinCEN reported 1,251 ransomware-related incidents at U.S. banks in 2021—which is more than double the 602 ransomware events reported in 2020. Further, the total value of these ransomware events in 2021 was about $886 million, which was 68 percent more than in 2020 ($527 million).

Further, 74 percent of bank leaders surveyed stated that their institution had experienced one or more ransomware attacks, with 63 percent of institutions paying the ransom demanded, according to VMWare.[21] Banks incur significant costs from ransomware attacks (beyond paying the ransom), including "data restoration, investigation and response, regulatory and legal fines, and brand damage."[22] In March 2022, a bank in New York suffered a cybersecurity incident—including ransomware and denial of service attacks—that resulted in the bank's temporary loss of access to its internal systems and data, and the exfiltration of bank customers' personal information.[23]

The Federal Reserve Board reported that cybersecurity risks may affect financial stability, because traditional stabilizing responses (capital and liquidity) are not likely to resolve such an attack. The Federal Reserve Board further noted that interconnected payment and settlement systems make it difficult to restore operations after a cybersecurity incident. As a result, "[u]ncertainty about the nature and extent of an incident may prompt runs on [the bank's] counterparties, competitors, or unaffected segments of the firm's operations."

The Office of the Comptroller of the Currency (OCC) also has observed "increases in the frequency and severity of cyber attacks against financial institutions and their service providers in recent years. Disruptive and destructive cyber attacks, such as ransomware, targeted at the financial sector have elevated risks beyond the mere threat of financial loss. Disruption to financial services can significantly impact banks' abilities to deliver critical services to their customers and has the potential to affect the broader economy."[24]

In its 2022 Risk Review, the FDIC stated that "[m]alicous cyber actors pose serious risk to bank information systems by compromising the security of software and computing services provided by third-party suppliers." The OCC further recognized that "[t]hreat actors are increasingly

exploiting vulnerabilities in IT systems and third-party software to conduct malicious cyber activities while negotiating ransom payments."[25] In April 2022, VMWare reported that "[c]ybercrime cartels have studied the interdependencies of financial institutions and now understand which managed service provider is used."[26] Sixty percent of the financial institutions in its survey were infiltrated through their vendor relationships or third-party service providers (TSP), a 58-percent increase from 2020, according to VMWare.[27] In May 2022, the Department of Homeland Security, Cybersecurity & Infrastructure Security Agency, issued an alert, Protecting Against Cyber Threats to Managed Service Providers and their Customers, stating that malicious cyber actors were targeting service providers to "enable follow-on activity—such as ransomware and cyber espionage—against the [service provider] and the [service provider's] customer base."

FDIC IT examinations should evaluate banks' IT risk management, to ensure that bank and TSP cybersecurity risks are mitigated.

Ensuring FDIC Examinations Address Cybersecurity Risks at Banks

The FDIC uses the Information Technology Risk Examination (InTREx) Program procedures to conduct risk-focused examinations to assess banks' management of IT and cybersecurity risks. The FDIC should ensure that its InTREx examinations accurately capture current and relevant risks and reflect the scope and complexity of banks' IT security and systems. The FDIC should also ensure that it has appropriate examination processes, resources, and staff. FDIC examiners should have up-to-date information on cyber controls and threats, and the requisite skills to identify risks and complete thorough examinations.

In our OIG evaluation, Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program (January 2023), we found weaknesses in the InTREx program that limit the ability of FDIC examiners to assess and address banks' IT and cyber risks at financial institutions:

- The InTREx program is outdated and does not reflect current Federal guidance and frameworks for three of four InTREx Core Modules;
- The FDIC did not communicate or provide guidance to its examiners after updates were made to the program;
- FDIC examiners did not complete InTREx examination procedures and decision factors required to support examination findings and ratings;
- The FDIC has not employed a supervisory process to review IT workpapers prior to the completion of the examination, in order to ensure that findings are sufficiently supported and accurate;
- The FDIC does not offer training to reinforce InTREx program procedures to promote consistent completion of IT examination procedures and decision factors;
- The FDIC's examination policy and InTREx procedures were unclear, which led examiners to file IT examination workpapers in an inconsistent and untimely manner;
- The FDIC does not provide guidance to examination staff on reviewing threat information to remain apprised of emerging IT threats and those specific to financial institutions;
- The FDIC is not fully utilizing available data and analytic tools to

improve the InTREx program and identify emerging IT risks; and

- The FDIC has not established goals and performance metrics to measure its progress in implementing the InTREx program.

The weaknesses detailed above collectively demonstrate the need for the FDIC to take actions to ensure that its examiners effectively assess and address IT and cyber risks during IT examinations. Without effective implementation of the InTREx program, significant IT and cyber risks may not be identified by examiners and addressed by financial institutions. We made 19 recommendations to the FDIC to improve its InTREx examination processes. The FDIC concurred with 16 of the 19 recommendations and partially concurred with 3 recommendations. Of the 19 recommendations, 5 are unresolved. We will work with the FDIC to reach resolution during the audit follow-up process.

Also, the FDIC faces an upcoming wave of pending retirements among its IT subject matter experts. As described later in this Top Challenges Report, 36 percent of examiners with advanced IT skills and 20 percent of IT examiners with intermediate skills were eligible to retire in 2022. These retirement-eligibility figures rise to 64 percent for advanced IT examiners and 44 percent for intermediate IT examiners in 2027. Absent skilled IT examiners, the FDIC may not have the expertise to identify banks' IT risks. The FDIC will need to replace this expertise in order to ensure it has the requisite number of skilled staff to complete IT examinations.

Examining for Third-Party Risk

Banks routinely rely on TSPs for numerous activities, including document processing, IT services, accounting, compliance, human resources, and loan servicing.[28] According to the FDIC's Supervisory Insights, "[f]ailure to manage [third-party] risks can expose a financial institution to regulatory action, financial loss, litigation, and reputational damage, and may even impair the institution's ability to establish new or service existing customer relationships."

In the Semiannual Risk Perspective (Fall 2022), the OCC noted that banks are increasingly reliant on TSPs, and that such dependence poses operational and cyber risks to banks. Numerous banks may rely on the services of at least one TSP, which increases the risk of a cyber incident passing from a TSP to other banks, or from one bank through a TSP to multiple banks. Further, the OCC stressed the importance of banks conducting due diligence and ongoing monitoring and oversight of TSPs "commensurate with the nature and criticality of the proposed activity."

FDIC examinations of banks' cybersecurity should include an assessment of the risk management programs of all TSPs affiliated with the bank. The Federal Financial Institutions Examination Council's (FFIEC) guidance, Supervision of Technology Service Providers, notes that "[a] financial institution's use of a TSP to provide needed products and services does not diminish the responsibility of an institution's board of directors and management to ensure that the activities are conducted in a safe and sound manner and in compliance with applicable laws and regulations just as if the institution were to perform the activities in-house." We have work planned to assess the FDIC's examination processes for TSPs.

Recording and Assessing Banks' Cybersecurity Incidents

The FDIC, along with other banking regulators, promulgated a rule requiring banks to notify the FDIC about certain computer security incidents within 36 hours of the event; this rule became effective on May 1, 2022.[29] According to the rule, the

banks must notify the primary bank regulator when a computer-security incident materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, a banking organization's ability to carry out its banking operations, the bank's business lines, or operations.[30]

According to FDIC data, between May 1 and July 31, 2022, banks reported 41 cybersecurity incidents under the new rule.[31] FDIC examinations should have procedures to evaluate banks' compliance with the regulatory requirements and identify possible underreporting of incidents. When FDIC personnel become aware of cybersecurity incidents at banks, they should report the information to law enforcement, including the FDIC OIG, for further investigation. As of the writing of this Top Challenges Report, the FDIC has not reported these cybersecurity incidents to law enforcement.

In addition, the FDIC does not currently have processes in place to ensure that reported incidents are recorded in the FDIC's system that supports FDIC supervision and insurance responsibilities called ViSION.[32] For example, a recent internal FDIC review of nine reported incidents at the Atlanta Regional Office found that four of the nine incidents reported to the FDIC were not recorded in the ViSION system.

In addition, it is critical that IT examiners are notified of banks' cybersecurity incidents, including the range of cybersecurity incidents occurring across FDIC-insured institutions. The FDIC should also look across all reported incidents for important trends and patterns of nefarious activity. Such trends may be helpful to examiners, policymakers, and banks as they assess cybersecurity risks at financial institutions.

Cybersecurity is a threat to banks and TSPs. A single cybersecurity incident—either alone or through interconnections—could have a devastating impact on financial stability in the United States. FDIC IT examinations should assess emerging cyber risks and ensure that banks and TSPs take appropriate action to address these risks. Further, the FDIC should have effective processes for the intake and assessment of banks' reporting of cybersecurity incidents, including follow-up to ensure their mitigation.

Supervising Risks Posed by Digital Assets

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Regulating digital assets in a coordinated fashion;
- Evaluating and supervising risks at banks related to digital assets; and
- Clarifying consumer risks regarding digital assets.

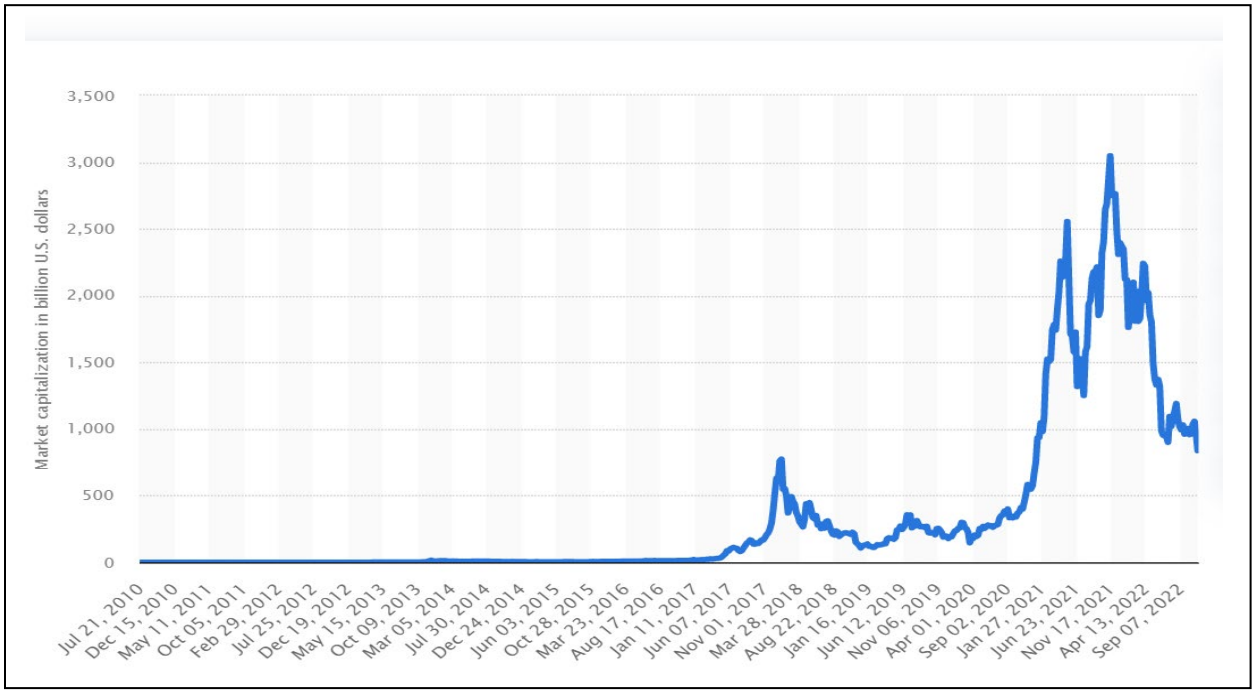
The OIG has identified Digital Asset Risk as a Top Challenge for the FDIC since 2018.

The Executive Order on Ensuring Responsible Development of Digital Assets (March 9, 2022), defined digital assets as a broad term including central bank digital currencies, crypto assets (also known as cryptocurrencies), and stablecoins that are used to "make payments or investments, or transmit or exchange funds or the equivalent thereof, that are issued or represented in digital form through the use of distributed ledger technology." The crypto asset markets have been extremely volatile over the last 3 years. The total market capitalization of crypto assets fluctuated from about $132 billion in January 2019 rising to $3 trillion in November 2021, and falling by about two-thirds to $1 trillion in 10 months (September 2022). As of December 2022, crypto asset market capitalization fell further to $840 billion.[33]

According to FDIC data, as of January 2023, the FDIC was aware that 136 insured banks had ongoing or planned crypto asset-related activities. For example, these banks have arrangements with third parties that allow bank customers to buy and sell crypto assets. Banks also provide account deposit services, custody services, and lending to crypto asset exchanges.

For example, it was reported that 90 percent of Silvergate Bank's deposit base

Figure 1: Crypto Asset Market Capitalization—July 2010 to September 2022



Source: Statistia.

(approximately $11.9 billion) were accounts for crypto asset customers.[34] In the 4th quarter of 2022, Silvergate Bank crypto asset customers withdrew funds causing total bank deposits to fall to $3.8 billion—a 68-percent deposit reduction from $11.9 billion in the 3rd quarter.[35] As a result, the bank was forced to quickly raise funds to satisfy customer withdrawals. The bank sold $5.2 billion in debt securities at a loss of $718 million, which is greater than the bank's total profits since about 2013. Further, the recent bankruptcy of crypto asset exchange FTX revealed that 11 banks were doing business with FTX and may have had involvement in alleged wire transfer fraud – this includes Moonstone Bank, where an FTX-affiliated company invested $11.5 million, doubling the bank's asset size of $5.7 million.[36] Banks also sponsor debit cards and prepaid cards that provide bank customers with crypto asset rewards.

Banks' interactions with crypto assets present risks for the FDIC in supervising banks and resolving failed institutions. The FSOC Report on Digital Asset Financial Stability Risks and Regulation (FSOC Digital Asset Report) (September 2022) noted that "[c]rypto-asset activities could pose risks to the stability of the U.S. financial system." For example, the Basel Committee on Banking Supervision noted that crypto asset price volatility could lead to bank "liquidity risk, credit risk, market risk, operational risk (including fraud and cyber risks), money laundering/terrorist financing risk, and legal and reputation risks."[37]

Banks must regularly assess the fluctuations in crypto asset values used as collateral. Further, the FDIC should maintain expertise in digital assets in order to manage bank resolutions for failed institutions. FinCEN also noted that the anonymity, lack of transparency, and speed of crypto assets made the use of crypto assets appealing for "money laundering, sanctions evasion, and other illicit financing."[38]

Executive Order 14067, Ensuring Responsible Development of Digital Assets (March 9, 2022), recognized that digital asset growth has "profound implications" for the protection of consumers, including data privacy and security, and criminal activity. According to the Comprehensive Framework for Responsible Development of Digital Assets, 16 percent of Americans (about 52 million people) have purchased digital assets. The Federal Trade Commission reported that since 2021, 46,000 people have lost over $1 billion to crypto asset scams.[39] As noted in the Joint Statement on Crypto-Asset Risks to Banking Organizations (January 3, 2023), the FDIC and other banking regulators should assess banks' crypto asset activities to ensure adequate safety and soundness, consumer protection, legal permissibility, and compliance with applicable laws and regulations, including anti-money laundering and illicit finance statutes and rules.

Regulating Digital Assets in a Coordinated Fashion

The FSOC Digital Asset Report noted that the current digital asset regulatory landscape was opaque. FSOC noted that there should be a consistent regulatory framework for digital assets, including the "analysis, monitoring, supervision, and regulation of crypto-asset activities." FSOC recommended a Government-wide approach to the collection and sharing of data to enhance regulators' understanding of digital assets in order to assess their impact on U.S. financial stability. Executive Order 14067, Ensuring Responsible Development of Digital Assets, also emphasized the importance of a "whole-of-government approach to addressing the risks and harnessing the potential benefits of digital assets and their underlying technology."

Prior to the FSOC Digital Asset Report and the Executive Order, on November 23, 2021, the Federal Reserve Board, the FDIC,

and the OCC issued a Joint Statement on Crypto-Asset Policy Sprint Initiative and Next Steps (Joint Statement) that "focused on quickly advancing and building on the agencies' combined knowledge and understanding related to banking organizations' potential involvement in crypto-asset-related activities" and provided a roadmap for agencies to collectively provide greater clarity on banks' crypto-related activities. The Joint Statement noted that "it is important that the agencies provide coordinated and timely clarity where appropriate to promote safety and soundness, consumer protection, and compliance with applicable laws and regulations, including anti-money laundering and illicit finance statutes and rules."

The recent Joint Statement on Crypto-Asset Risks to Banking Organizations (January 3, 2023), noted risks for digital assets, including fraud, legal uncertainty regarding custody and crypto asset ownership rights, unfair or misleading representations and disclosures regarding deposit insurance by crypto asset firms, crypto asset volatility and contagion risk from crypto asset interconnections, and potential banking outflow and stability risks for stablecoins. Regulators stated that they "continue to take a careful and cautious approach related to current or proposed crypto-asset-related activities and exposures at each banking organization." We have ongoing work to determine whether the FDIC has developed and implemented strategies that address the risks posed by crypto assets.

Evaluating and Supervising Risks at Banks Related to Digital Assets

Criminals use crypto assets for illicit activities and move funds to conceal or disguise the origin of funds.[40] The FDIC should ensure that its examiners have the appropriate training, skills, and processes to assess crypto asset risks at banks.[41] The FDIC also should have resolution staff with the appropriate skillsets and processes to resolve banks involved in digital assets. Otherwise, examiners may be unaware of banks' digital asset risks, and FDIC resolution and asset sales may be impacted by a bank's digital-asset holdings or activities.

In addition, FDIC examination, receivership, and other staff overseeing digital-asset supervision and policy should be free from any conflicts of interest. On July 5, 2022, in a Legal Advisory, the Office of Government Ethics stated that a Federal "employee who holds any amount of a cryptocurrency or stablecoin may not participate in a particular matter if the employee knows that particular matter could have a direct and predictable effect on the value of their cryptocurrency or stablecoins." On August 17, 2022, the FDIC issued an Ethics Analysis that allows employees with certain interest in digital assets to participate in non-policymaking assignments. For example, if an employee holds the crypto asset Ethereum, the employee may examine a bank that is involved in Bitcoin provided the effect of the examination does not go beyond Bitcoin. As banks increase their involvement with crypto assets, the FDIC should ensure that it has sufficient staff that are not conflicted in order to meet its mission requirements.

Clarifying Consumer Risks Regarding Digital Assets

According to the Comprehensive Framework for Responsible Development of Digital Assets, approximately 52 million Americans have purchased digital assets. The FDIC has noted an "increasing number of instances where financial service providers or other entities or individuals have misused the FDIC's name or logo or have made false or misleading representations about deposit insurance."[42] For example, bankrupt crypto asset platform Voyager Digital (Voyager) misrepresented that U.S. dollars deposited with the firm for the purchase of crypto assets were covered by FDIC insurance. Voyager had deposit

accounts for the benefit of its customers at Metropolitan Commercial Bank that were used for customers' purchase and sale of crypto assets, but Voyager was not FDIC-insured.[43] Voyager customers have not received their funds and await bankruptcy court rulings regarding potential fund recovery.[44]

The FDIC became aware of Voyager's misrepresentation of FDIC insurance in February 2021. However, it was not until 17 months later on July 28, 2022, that the FDIC and the Federal Reserve Board issued a letter demanding that Voyager cease and desist from making false and misleading statements regarding its FDIC deposit insurance status and take immediate action to correct any such prior statements.[45] One day after issuing the joint letter to Voyager, the FDIC noted its concerns about the risks of consumer confusion or harm arising from crypto assets offered in connection with insured depository institutions.[46] On August 19, 2022, the FDIC issued additional cease and desist letters to five companies for making crypto-related false or misleading representations about deposit insurance.[47]

The risks associated with digital assets and emerging technologies require a whole-of-government response. FDIC digital asset guidance for banks and policies and procedures for examinations should be consistent with those of other regulators to ensure that similarly situated banks are subject to the same supervisory strategies. The FDIC should also have information and analysis regarding digital asset risks to make data-driven policy decisions and enable broad assessment of risks across the banking sector.

Fostering Financial Inclusion for Underserved Communities

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Developing the FDIC's strategy to foster financial inclusion; and
- Managing bias risk associated with technology.

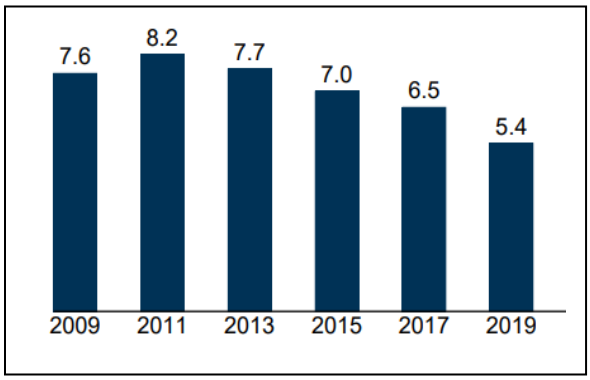
The OIG has identified Financial Inclusion as a Top Challenge since 2020.

The World Bank notes that access to a bank account is "a first step toward broader financial inclusion since a transaction account allows people to store money, and send and receive payment."[48] In addition, bank accounts allow previously excluded and underserved populations to receive other financial products.

Developing the FDIC's Strategy to Foster Financial Inclusion

In October 2022, the FDIC, in partnership with the Census Bureau, issued its biennial 2021 National Survey of Unbanked and Underbanked Households. The Survey found that 5.4 percent were unbanked—meaning that no one in the household had a checking or savings account at a bank or credit union (Figure 2).

Figure 2: Household Unbanked Percentage Rate, 2009-2021

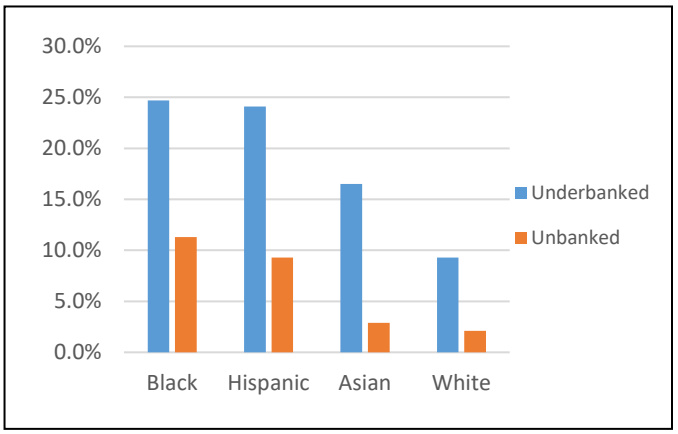


Source: FDIC 2021 National Survey of Unbanked and Underbanked Households (October 2022).

Further, the Survey found that 14.1 percent were underbanked—meaning that someone in the household had a bank account, but they used other high-cost services, such as money orders, check cashing, payday lending, pawn shops, tax refund anticipation loans, or auto title loans.

The Survey also found disparities in banking status based on race and ethnicity. As shown in Figure 3, consistent with prior surveys, the unbanked and underbanked rates were higher for Black, Hispanic, and Asian households than for White households. Further, the Federal Reserve Board found that on average, Black and Hispanic households earned half of White households and that their net worth was 15 to 20 percent of White households.[49]

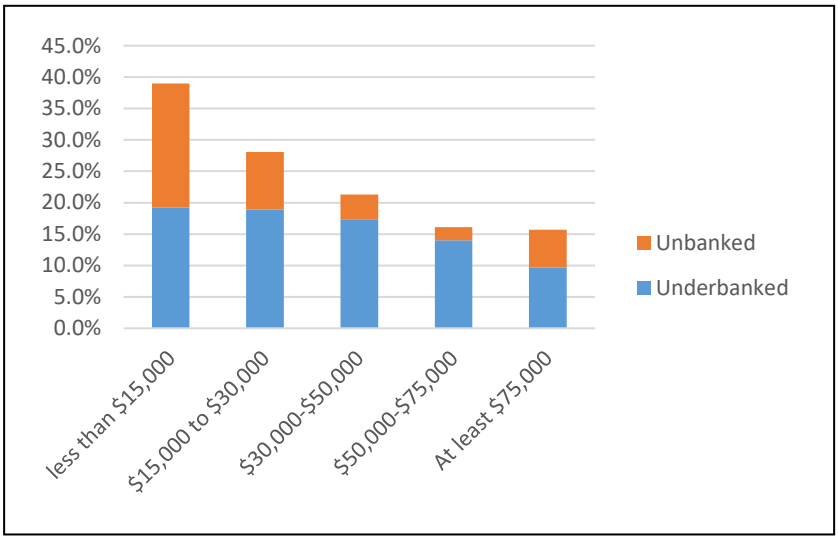
Figure 3: Banking Status by Race/Ethnicity



Source: FDIC 2021 National Survey of Unbanked and Underbanked Households (October 2022).

In addition, the Survey noted differences based on household income. As shown in Figure 4, consistent with prior Surveys, households with lower income had higher unbanked and underbanked rates when compared to households with incomes of $50,000 or more.

Figure 4: Unbanked and Underbanked Rates by Household Income



Source: FDIC 2021 National Survey of Unbanked and Underbanked Households (October 2022).

The FDIC has identified financial inclusion as a strategic challenge for the Agency.[50] Further, the FDIC has not completed development of measures to determine the effectiveness of its efforts to promote financial inclusion, including whether it is achieving the desired outcomes.

The Government Accountability Office (GAO) reported that the FDIC's plans (Economic Inclusion Strategic Plan and Annual Performance Plan) do not assess the outcomes of efforts to facilitate consumers' access to banking services.[51] In February 2022, the GAO recommended that the FDIC develop and implement outcome-oriented performance measures for its strategic objective of ensuring access to safe and affordable bank services that reflect leading practices, including demonstrating results, measuring outcomes, and providing useful information for decision-making. The FDIC's 2022 Annual Performance Plan included a goal to track and report outcome-based performance measures for economic inclusion programs; however, the GAO recommendation remains unimplemented at the time of this Report.

Absent outcome-oriented performance measures for financial inclusion-related work, the FDIC is limited in evaluating whether these programs and initiatives are effective in increasing participation in the insured banking system. We have ongoing work to determine whether the FDIC has developed and implemented an effective strategic plan to increase participation in the banking system.

Managing Bias Risk Associated with Technology

In October 2022, the White House Office of Science and Technology Policy issued a Blueprint for an AI Bill of Rights that identified five principles and associated practices to help guide the design, use, and deployment of automated systems to protect the American public in the age of Artificial Intelligence (AI).[52] These principles include: Protection from unsafe or ineffective automated systems; Protection from discrimination by algorithms and systems; Data privacy; Explanation of how an automated system is being used and why it contributes to outcomes; and Access to personnel who will remedy problems encountered. While AI can offer banks certain benefits, it can generate or amplify risks to consumers, such as unlawful discrimination; unfair, deceptive, or abusive acts or practices; and privacy concerns. In particular, AI models may use data that has inherent biases, and its models may be outdated without proper oversight.[53]

In May 2022, a working paper from the Federal Reserve Bank of Minneapolis found bias in conventional mortgage data processed between 2018 and 2020. Specifically, data indicates that Black applicants were 2.9 percent more likely to have their mortgage denied than White applicants, and Asian and Latinx applicants were 2.2 percent and 1.5 percent more likely to face denials, respectively, than White applicants. The study concluded that biased systems and data can adversely affect minority communities.

On March 31, 2021, the FDIC and other financial regulators issued a Request for Information (RFI) to gather information and public comments on financial institutions' use of AI, including machine learning. The purpose of this RFI was to understand respondents' views on the use of AI by financial institutions in their provision of services to customers and for other business or operational purposes. On May 17, 2021, the RFI comment period was extended from June 1, 2021 to July 1, 2021. Although the FDIC has stated that it has engaged with other regulators on this topic, as of the date of this Top Challenges Report, the FDIC has not promulgated AI policy guidance.

Also, in a November 29, 2021 letter, the Chairwoman of the House Financial Services Committee and Chairman on the Task Force on Artificial Intelligence requested that the FDIC, in assessing banks' use of AI, "prioritize principles of transparency, enforceability, privacy, and fairness and equity … [to] ensure AI regulation and rulemaking can meaningfully address appropriate governance, risk management, and controls over AI."

The FDIC should ensure that it takes a holistic, outcome-based approach in its efforts to address unbanked and underbanked individuals. This may include new methods or strategies to reach Black, Hispanic, Asian, and low-income communities. Further, FDIC examinations should ensure that banks' decision-making technologies and analytics are unbiased measures of creditworthiness.

Fortifying IT Security at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Improving the FDIC's information security profile;
- Protecting the FDIC's wireless network;
- Assessing the FDIC's readiness for a ransomware attack;
- Migrating the FDIC's IT systems to the cloud;
- Addressing weaknesses in the FDIC's personnel security program; and
- Ensuring the security and privacy of FDIC information.

The OIG has identified IT Security as a Top Challenge for the FDIC since 2018.

According to the Cybersecurity & Infrastructure Security Agency (CISA), the Federal Government must improve its efforts to protect against malicious cyber campaigns to ensure the security of Federal IT assets.[54] In 2022, the GAO continued to recognize Federal IT security as a high risk across the Federal Government,[55] and in 2021, Federal IT systems suffered 32,543 incidents, a 6-percent increase from 2020.[56]

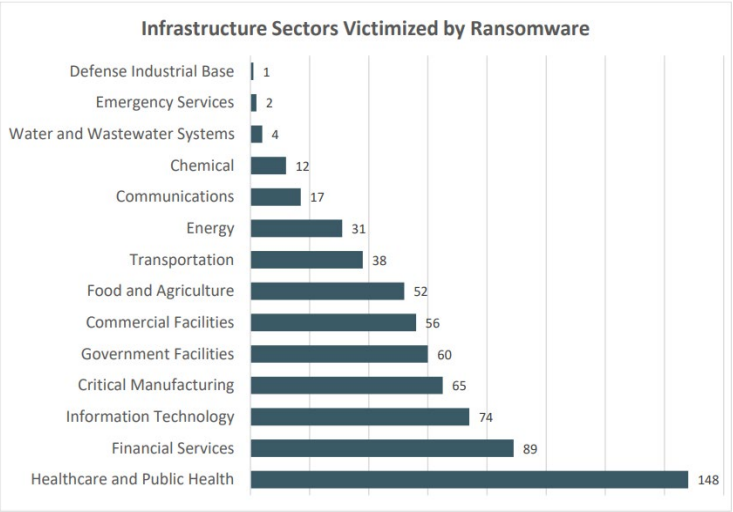
For example, on November 16, 2022, CISA issued an alert that the network of a Federal agency was compromised by Iranian Government-sponsored actors.[57] The threat actors exploited unpatched vulnerabilities in a certain proprietary server, were able to move laterally throughout the network, compromised credentials, and installed mining and other software.

CISA further noted that IT and cyber vulnerabilities used to exploit private organizations, as shown in Figure 5, pose similar risks to Federal agencies.[58]

According to a report from cybersecurity firm Comparitech, there were 330 ransomware attacks on state and local government organizations between 2018 and October 2022 that impacted data for over 230 million individuals with ransom demands totaling $36.5 million. For example, in August 2022, the City of Wheat Ridge, Colorado was attacked by ransomware, and the town refused to pay the ransom. It took more than 3 weeks to determine whether the town could resume operations through backup data.

The FDIC relies heavily on information systems, data, and personnel to carry out its mission. The FDIC is custodian of about 1.8 petabytes of sensitive and Personally Identifiable Information (PII) relating to failed banks and more than 4,700 insured banks. FDIC IT systems also contain sensitive information, such as PII that includes names, Social Security Numbers, and bank account numbers for FDIC employees and depositors of failed financial institutions; confidential bank examination information, including supervisory ratings; and sensitive financial data, including credit card numbers.

Figure 5: Infrastructure Sectors Victimized by Ransomware



Source: FBI Internet Crimes Complaint Center.

The FDIC should have effective controls in place to protect the information contained in its IT systems. The FDIC has a duty to ensure the safekeeping of sensitive information and PII that it collects, maintains, uses, and discloses.[59] A cybersecurity incident at the FDIC could severely limit its capabilities to meet mission requirements, particularly during a crisis.

The FDIC should also ensure that its employees and contractors possess the requisite suitability to ensure the safety and security of the FDIC workplace and information. An FDIC data breach could result in FDIC employees and contractors, bank customers, and bank employees and executives suffering identity theft, and affected banks and the FDIC experiencing operational and reputational risk.

Improving the FDIC's Information Security Profile

In our OIG report, The FDIC's Information Security Program –2022 (September 2022), we evaluated the effectiveness of the FDIC's information security program and practices. We found security control weaknesses that reduced the effectiveness of the FDIC's information security program and practices:

- **The FDIC's Supply Chain Risk Management (SCRM) Program Lacks Maturity:** The FDIC is still developing its policies and procedures to address the SCRM finding from our Information Security report in 2021. Additionally, in our OIG evaluation report, The FDIC's Implementation of Supply Chain Risk Management (March 2022), we found that the FDIC had not implemented several objectives outlined in its SCRM Implementation Project Charter; did not conduct supply chain risk assessments in accordance with best practices; had not ensured that its Enterprise Risk Management processes fully capture supply chain risks; and FDIC Contracting Officers did not maintain contract documents in the proper system. We issued nine recommendations, five of which remain unimplemented.

- **The FDIC Did Not Adequately Oversee and Monitor Information Systems:** Federal agencies must conduct security risk assessments for the information and information systems that support the operations and assets of the agency, including those provided or managed by contractors and other entities. We concluded that the FDIC had not conducted security risk assessments in accordance with National Institute of Standards and Technology (NIST) guidance for approximately 52 percent of its legacy systems and subsystems (as of May 19, 2022).

- **The FDIC Did Not Address Flaw Remediation Plans of Action and Milestones (POA&M) in a Timely Manner:** A POA&M is a 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. We found that the FDIC had 31 POA&Ms related to flaw remediation open past their estimated completion dates (as of June 21, 2022).

- **The FDIC Did Not Configure Privileged Accounts in Accordance with the Principle of "Least Privilege":** We are currently conducting an audit of the FDIC's security controls over its Windows Active Directory. During the course of our work, we identified instances where accounts were configured with elevated account settings;

however, there was no justification provided for such settings, and the elevated settings were no longer needed for administrators to perform their business roles. Additionally, we identified concerns relating to the Background Investigations for Privileged Account Holders at the FDIC and issued a Management Advisory Memorandum in June 2022.

- **The FDIC Did Not Fully Implement Its Document Labeling Guide:** In a previous OIG report, The FDIC's Information Security Program - 2021, we recommended that the FDIC implement document labeling guide requirements across the organization. However, the FDIC had not yet implemented this recommendation and did not anticipate implementation until 2023.

These control weaknesses must be improved to reduce the impact to the confidentiality, integrity, and availability of the FDIC's information systems and data.

Protecting the FDIC's Wireless Network

The FDIC provides wireless access (WiFi) throughout its facilities. Absent effective security controls, WiFi access provides an avenue into FDIC systems that could compromise the confidentiality, availability, and integrity of FDIC data and systems. In our OIG review of Security Controls Over the FDIC's Wireless Network (December 2022), we found that the FDIC did not comply or partially complied with five practices recommended by NIST and guidance from the FDIC and other Federal agencies in the following areas:

- **Configuration of Wireless Networks:** The FDIC did not properly configure its Policy Manager, which enforces security policies for wireless network connectivity. Also, the FDIC's Chief Information Officer Organization's (CIOO) Wi-Fi Operations Group did not have control or awareness of the set-up and configuration of numerous wireless devices operating in FDIC buildings and facilities.

- **Wireless Signal Strength:** The FDIC did not have processes to examine and modify the signal strength of wireless devices and networks broadcasting throughout its buildings and leaking outside of FDIC facilities.

- **Security Assessments and Authorizations:** The FDIC did not maintain a current Authorization to Operate for its wireless network and did not conduct sufficient continuous monitoring testing activities to support the Agency's ongoing authorization of its wireless network.

- **Vulnerability Scanning:** The FDIC did not include certain wireless infrastructure devices in its vulnerability scans. In addition, the FDIC did not use credentialed scans on wireless infrastructure devices.

- **Wireless Policies, Procedures, and Guidance:** The FDIC did not maintain policies and procedures addressing key elements of the FDIC's wireless networks, including roles and responsibilities for the CIOO's Wi-Fi Operations Group; procedures for remediating wireless equipment alerts; standards for configuration settings; updates of wireless inventory records; and detection of rogue access points.

As a result, the FDIC faces potential security risks based upon its current wireless practices and controls, including

unauthorized access to the FDIC networks and insecure wireless devices broadcasting Wi-Fi signals. We made eight recommendations to strengthen FDIC wireless networks.

Assessing the FDIC's Readiness for a Ransomware Attack

According to CISA, "[r]ansomware is an ever-evolving form of malware designed to encrypt files on a device, rendering any files and systems that rely on them unusable." The goal of most ransomware attacks is to halt processes, interrupt services, and cause disruption until a ransom payment is made in exchange for decrypting files and systems. CISA notes that ransomware "can severely impact business processes and leave organizations without the data they need to operate or deliver mission-critical services."

The FDIC relies on its IT systems for day-to-day activities and especially during crises. A ransomware attack on the FDIC could hinder the FDIC's ability to resolve failed banks, issue deposit insurance payments to bank account holders, examine and supervise financial institutions, and manage receiverships. Disruption of any of these FDIC core functions could lead to financial system instability, including a loss of public confidence in the FDIC's ability to pay depositors. We have work planned to assess the FDIC's activities to prepare for and respond to a ransomware attack.

Migrating the FDIC's IT Systems to the Cloud

Executive Order 14028, Improving the Nation's Cybersecurity, requires Federal agencies to adopt security best practices, including accelerating the transition of IT systems to secure cloud environments. Cloud transition requires the secure and effective transfer of data from legacy systems into new cloud environments hosted by outside organizations. According to the GAO, Federal agencies face four key risks in their cloud transitions:

- Ensuring the cybersecurity of cloud service providers.
- Procuring cloud services through agreements that define security breaches and responsibilities, how data will be managed, and the possible consequences for non-compliance with the agreement.
- Maintaining a skilled workforce for a cloud environment.
- Tracking cloud transition costs and savings.[60]

The FDIC accelerated its multi-year transition to a cloud-based environment and has spent over $100 million on this effort since 2021. The FDIC should ensure that it safeguards FDIC data and information during the cloud transition. FDIC cloud computing contracts should include information security provisions, and the FDIC should have knowledgeable staff and governance processes to manage these contracts. We have ongoing work to assess the governance, strategy, and security of the FDIC's cloud-based systems.

Addressing Weaknesses in the FDIC's Personnel Security Program

According to the 2022 Verizon Data Breach Investigations Report, data breaches involving misuse of access are almost entirely conducted by insiders. To protect FDIC personnel, systems, and information, the FDIC vets all employees and contractors for standards of fitness and integrity and conducts background investigations commensurate with an individual's duties.[61] The FDIC's personnel security and suitability program is the first line of defense to ensure a safe workplace and to mitigate the risk of unauthorized IT access to FDIC sensitive information and PII.

In our OIG Management Advisory Memorandum, Background Investigations for Privileged Account Holders (June 6, 2022), we identified that the FDIC did not have adequate controls to ensure that certain contractors and employees who require privileged access to FDIC information systems and data had background investigations commensurate with their positions. As a result, the FDIC could not be sure that certain employees and contractors who were granted privileged access to the FDIC's information systems and related data subsequent to their onboarding would have an appropriate risk designation level and related background investigation. The FDIC took actions to address our findings.

In 2021, we also found several deficiencies in the FDIC's background investigation program. In our OIG evaluation, The FDIC's Personnel Security and Suitability Program (January 2021), we concluded that the FDIC's program was not fully effective in ensuring the timely completion of preliminary suitability screenings, background investigations commensurate with position risk designations, and reinvestigations. Specifically we found that two contractors with IT administrator rights remained with the FDIC despite unfavorable background adjudications. These individuals had access to FDIC databases and information for nearly 6 years and over 4 years, respectively. The FDIC took action to close the 21 recommendations from our report.

The FDIC should maintain and sustain controls over its personnel security program as it hires and transfers employees and contractors in a changing work environment.

Ensuring the Security and Privacy of FDIC Information

In recent reports, both the GAO and the OIG have found that the FDIC should strengthen controls to secure sensitive information and PII. The GAO found that the FDIC had "not established metrics to measure its overall implementation of privacy controls."[62] Absent such metrics, the FDIC is challenged to report on the sufficiency of its privacy controls. The GAO recommended that the FDIC identify and specify privacy metrics.

In our OIG report, The FDIC's Privacy Program (December 2019), we found that the FDIC's Privacy Program controls and practices we assessed were not effective or partially effective in four areas:

- 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;
- The FDIC did not adequately define the responsibilities of the Deputy Chief Privacy Officer or implement Records and Information Management Unit responsibilities for supporting the Privacy Program;
- The FDIC did not effectively manage or secure PII stored in network shared drives and in hard copy, or dispose of PII within established timeframes; and
- The FDIC did not ensure that Privacy Impact Assessments were always completed, monitored, and retired in a timely manner.

These 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. We made 14 recommendations that have been implemented by the FDIC.

The security of FDIC systems impacts bank employees and their customers, FDIC employees and contractors, and the U.S. financial sector. The FDIC should ensure that its IT security can withstand risks to Federal systems, including the increasing risks posed by ransomware and those posed when systems transition to the cloud. Further, the FDIC should have robust personnel security and suitability program and privacy controls to safeguard sensitive information and guard against insider threats. Strong IT systems ensure that the FDIC can securely carry out day-to-day activities and respond to crisis events.

Managing Changes in the FDIC Workforce

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Managing a wave of pending retirements at the FDIC; and
- Addressing increased resignations by examiners-in-training.

The OIG has identified FDIC Workforce Changes as a Top Challenge for the FDIC since 2019.

The GAO has recognized strategic human capital management as a high-risk area across the Federal Government. The FDIC faces challenges in the strategic management of its workforce. In 2022, more than 21 percent of the FDIC workforce was eligible to retire. Retirement-eligibility rates were higher for senior FDIC leaders and Subject Matter Experts, and in certain FDIC Divisions and Offices with critical roles for the Agency's Crisis Readiness. In addition, in 2021 and 2022, the FDIC experienced a substantial number of resignations among bank examiners-in-training—at rates greater than pre-pandemic levels. Examiners play key roles in assessing the safety and soundness of banks, and it is costly for the FDIC to hire and train replacement examiners.

The FDIC should ensure strategic management of its workforce and manage the loss of employees to retirements and resignations, while navigating its post-pandemic hybrid work environment where 80 percent of FDIC employees are working remotely. Without strategic workforce planning, retirements and resignations could result in the FDIC experiencing mission-critical skills and leadership gaps.

Managing a Wave of Pending Retirements at the FDIC

The FDIC's ability to execute its mission may be affected by numerous departures of its personnel. A total of 21 percent (1,264 individuals) of the FDIC workforce was eligible to retire in 2022 (Table 1); this figure is significantly higher than the Government-wide rate of 15 percent.[63] This retirement-eligibility figure climbs to more than a third of the FDIC workforce—-38 percent (2,215 individuals)—within 5 years (in 2027).

Table 1: FDIC Employee Retirement Eligibility Percentage

Division	2022 (%)	2027 (%)
Legal Division	39	50
Division of Finance (DOF)	39	49
Division of Resolutions and Receiverships (DRR)	36	54
Division of Administration (DOA)	28	45
Division of Risk Management Supervision (RMS)	18	34
Division of Information Technology (DIT)	16	33
Division of Insurance and Research (DIR)	16	30
Division of Depositor and Consumer Protection (DCP)	16	32
Division of Complex Institution Supervision & Resolution (CISR)	15	36
Overall for the FDIC	21	38

Source: OIG analysis of DOA retirement data as of June 2022.

Further, all FDIC Divisions have current retirement-eligibility rates that are greater than the 15-percent Government-wide average rate of retirement-eligibility.

Retirements in Key Crisis Readiness FDIC Divisions. The FDIC faces significant risks regarding retirement eligibility in key Divisions involved in Crisis Readiness efforts. In 2022, 36 percent of all employees in the Division of Resolutions and Receiverships were eligible to retire (Table 1). This figure rises to 54 percent in 5 years. DRR employees are critical in crises, because they work to resolve failed banks by arranging the sale of assets and liabilities to healthy banks, ensure timely payment of deposit insurance to bank customers when an acquiring bank is not found, and sell failed bank assets that are not sold at the time of resolution using a variety of sales strategies and techniques.

In addition, Divisions that support the FDIC's efforts to resolve failed banks also face significant retirement challenges. For example, the FDIC attorneys in its Legal Division execute documents to support the FDIC's failed bank transactions and investigate professional liability claims against failed bank management. In 2022, the Legal Division's retirement-eligibility rate was 39 percent and rising to half of the Division (50 percent) in 5 years. The Division of Finance and Division of Administration also play important roles during crises through the provision of deposit insurance and receivership funding, and contracting for goods and services, respectively. DOF had retirement-eligibility rates of 39 percent for 2022 and 49 percent in 5 years. DOA staff retirement-eligibility rates were 28 percent in 2022 and increased to 45 percent in 5 years. Absent seasoned professionals from key Divisions with institutional knowledge of lessons learned from past crises, the FDIC may not be able to execute its responsibilities with respect to resolution and receivership activities.

Retirements for FDIC Subject Matter Experts. In addition, nearly a third of FDIC employees who are considered Subject Matter Experts (SME) in risk areas related to consumer compliance matters, trusts, and IT were eligible to retire at the end of 2022 (Table 2). The FDIC designates certain personnel as SMEs because of the individuals' deep understanding and experience regarding certain functions or subject areas, and retirement rates for these experts climb within the next 5 years.

Table 2: FDIC Subject Matter Expert Employee Retirement Eligibility Percentage

SME Designation	2022 (%)	2027 (%)
Consumer Compliance	39	56
Trusts	32	55
Advanced IT	31	64
Intermediate IT	21	45
Bank Secrecy Act/Anti-Money Laundering (BSA/AML)	18	45
Accounting	16	37
Capital Markets	11	30

Source: OIG analysis of RMS and DCP SME data in combination with DOA retirement data as of June 2022.

The retirement-eligibility rates for FDIC Advanced and Intermediate IT SMEs escalates at a time when cyber threats at banks and their TSPs are increasing (as noted in the Mitigating Cybersecurity Risk at Banks and Third Parties section of this Report). In 2022, Advanced IT SME retirement-eligibility rates were 31 percent rising to 64 percent in 5 years. For Intermediate IT expertise, retirement-eligibility rates for 2022 were 21 percent and increasing to 45 percent in 5 years. Similarly, retirement-eligibility rates for FDIC Consumer Compliance experts is increasing.

Executive and Managerial Retirements. As noted in Table 3, a total of 40 percent of FDIC Executives and 30 percent of FDIC Managers were eligible to retire in 2022. These rates climb to 67 percent for FDIC Executives and 56 percent for Managers in 5 years.

These retirements may result in gaps in leadership positions. Leadership gaps can cause delayed decision-making, reduced program oversight, and failure to achieve Agency goals.

Table 3: FDIC Executives and Managers Retirement Eligibility Percentage

Regional Office	2022 (%)	2027 (%)
Executives		
Atlanta	50	100
Chicago	67	80
Dallas	60	80
Kansas City	75	75
New York	20	60
San Francisco	67	100
Headquarters	37	64
All EMs	40	67
Managers		
Atlanta	18	51
Chicago	23	64
Dallas	44	71
Kansas City	41	74
New York	17	49
San Francisco	29	57
Headquarters	30	49
All CMs	30	56

Source: OIG analysis of DOA retirement data as of June 2022.

Certain FDIC Regional Offices have significantly higher retirement rates for their Executives and Managers. For example, 75 percent of all Executives in Kansas City, and 60 percent or more of the Executives from the Chicago, Dallas, and San Francisco Regional Offices were eligible to retire in 2022.

Beginning in 2023, the FDIC's Atlanta Regional Office faces a 100-percent retirement-eligibility rate for its Executives. Further, over 40 percent of the Managers in the Dallas and Kansas City Regional Offices were eligible to retire in 2022.

Addressing Increased Resignations by Examiners-in-Training

The FDIC is also facing increasing resignation rates for its examiners-in-training known as Financial Institution Specialists (FIS). As shown in Figure 6, the FDIC saw more than a doubling of FIS resignations after 2020—with 54

resignations in 2021 and another 62 resignations for the first 9 months of 2022.

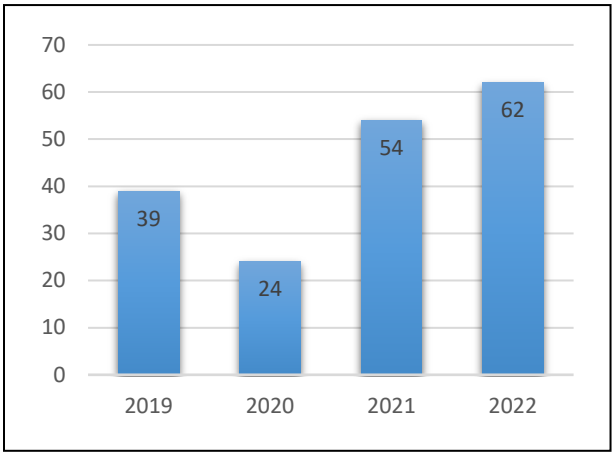
FIS resignations are costly to the FDIC. The FDIC invests in approximately 4 years of training from the time a FIS is hired until that individual earns an examination commission. Such commissioning requires that employees meet benchmarks, training, and other technical requirements, including passing a Technical Examination. Of the 62 FIS resignations in 9 months of 2022, 32 percent had 3 or more years of FDIC training, 53 percent had between 1 and 2 years of FDIC training, and 15 percent had less than one year of FDIC training. The total cost to train each new FIS is about $400,000.

Further, the departure of FIS personnel impacts FDIC succession planning and management. More than 17 percent of all current FDIC examiners were eligible to retire 2022, and this figure rises to 36 percent in 5 years (2027). Given the timeline for FIS training, the FDIC may have a limited number of new examiners to fill the positions of retiring seasoned examiners.

We had previously identified concerns with the FDIC's management of its employee retention, including a lack of established metrics or indicators to measure the effectiveness of its retention activities or actions for examination staff. In our OIG memorandum, The FDIC's Management of Employee Talent (September 2021), we found that the FDIC:

- Did not have clear goals to manage employee retention.

Figure 6: FIS Resignations by Year



Source: OIG analysis of DOA separation data 2019-September 2022.

- Did not have a systematic process for collecting and analyzing employee retention data. The FDIC did not have a systematic process to holistically capture and analyze data, and to ensure that the information flowed to the Divisions and Offices.
- Did not establish metrics or indicators to measure the effectiveness of its retention activities or actions. The FDIC could not determine whether or not its retention activities were working effectively.

We made three recommendations to improve the FDIC's management of talent at the Agency. One recommendation remains unimplemented as of the writing of this Top Challenges report.

The FDIC should continue to focus on managing its human capital lifecycle—hiring, talent management, resignations, and retirements.

Improving the FDIC's Collection, Analysis, and Use of Data

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Facilitating threat information sharing among financial sector participants; and
- Ensuring adequate data collection and analysis.

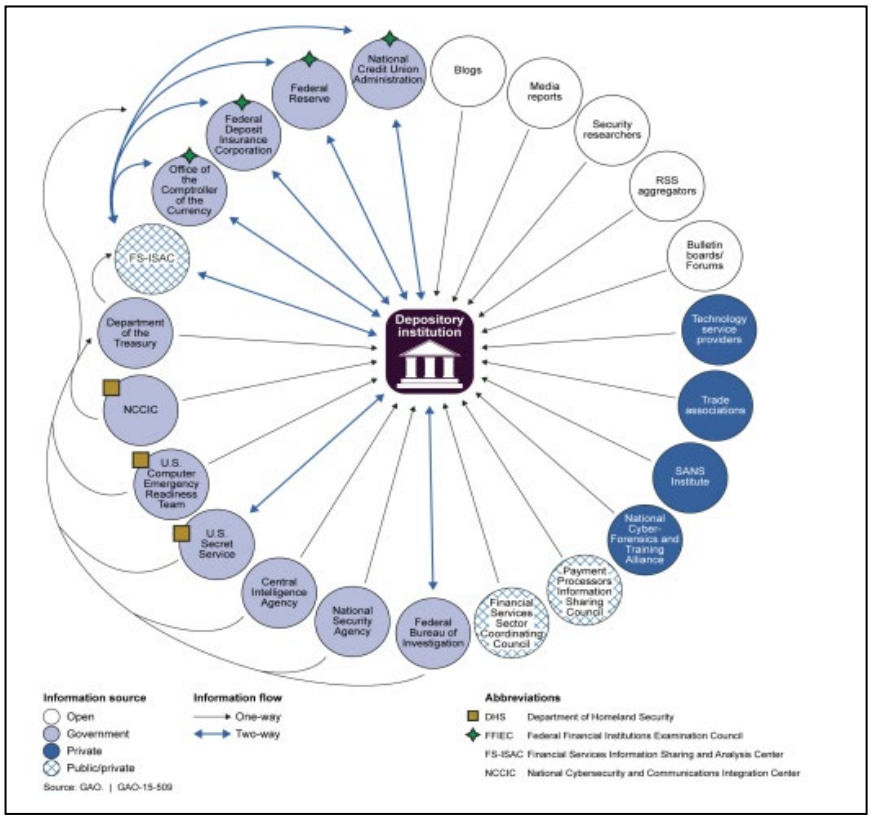
The OIG has identified Sharing of Threat Information as a Top Challenge for the FDIC since 2018.

Federal Government agencies gather a substantial volume of information related to financial institutions and their operations in the United States, and thus, relevant to FDIC supervisory and other activities. For example, Government agencies collect information about cyber threats, money laundering, and illicit financing activity.[64] Figure 7 depicts the GAO's determination of entities that hold information relevant to banks and the financial services sector.

The FDIC collects threat information relevant to the financial services sector regarding cyber attacks, money laundering, terrorist financing, pandemics, and natural disasters. Both the FSOC and OCC have encouraged greater information sharing among public and private entities to safeguard against threats to the financial sector.[65] Effective sharing of threat information helps the FDIC develop situational awareness, supports informed decision-making, enhances supervisory strategies, and assists in ensuring financial stability in the United States. According to NIST, information sharing also allows organizations to leverage "knowledge, expertise, and capabilities … to gain a more complete understanding of threats" and allows for informed decision-making.[66] Further, multiple sources of threat information can allow an organization to enrich existing information and make it actionable.

In addition, agencies may use data to understand and improve their programs and operations, and enable data-driven decision-making.[67] Federal agencies are also using sophisticated data analytics such as AI and machine learning. The FDIC should ensure that it receives and accesses actionable and relevant information regarding threats to the financial sector, analyzes such information, and shares it with its own Agency personnel and banks in order to mitigate the threats. The FDIC should also collect and analyze data in order to guide FDIC decision-making,

Figure 7: Sources of Threat Information for Financial Institutions

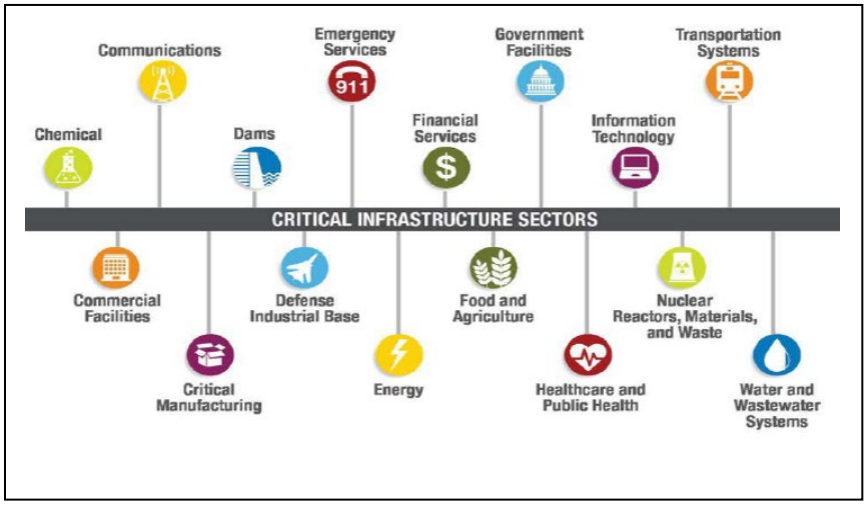


identify trends and patterns, and proactively address threats and vulnerabilities.

Facilitating Threat Information Sharing Among Financial Sector Participants

As shown in Figure 8, the FDIC is a member of the financial services sector, which is one of 16 critical infrastructure sectors with "physical and cyber systems and assets that are so vital to the United States that their incapacity or destruction would have a debilitating impact on our physical or economic security or public health or safety."[68]

Figure 8: 16 Critical Infrastructure Sectors in the U.S.



Source: DHS Critical Infrastructure Threat Sharing Framework, A Reference Guide for the Critical Infrastructure Community (October 2016).

In our OIG report, Sharing of Threat Information to Guide the Supervision of Financial Institutions (January 2022), we assessed whether the FDIC established effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. We found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. We identified gaps in the FDIC's Threat Sharing Framework. Specifically:

- The FDIC did not establish a written governance structure to guide its threat information sharing activities;
- The FDIC had not completed or implemented a governance Charter that established a common understanding of the role for the Intelligence Support Program or defined an overall strategy and requirements for it;
- The FDIC had not developed goals, objectives, or measures to guide the performance of its Intelligence Support Program;
- The FDIC did not establish adequate policies and procedures that defined roles and responsibilities for key stakeholders involved in the threat information sharing program and activities; and
- The FDIC did not fully consider the risks discussed in our report for its Enterprise Risk Inventory and Risk Profile.

We also identified gaps in the FDIC's processes for acquiring, analyzing, and disseminating threat information, and in its processes for obtaining feedback from stakeholders regarding how the use of threat information can be improved.

We made 25 recommendations to the FDIC to close these gaps and to ensure effective sharing of threat information to guide the FDIC's supervision of financial institutions. As of this Top Challenges Report, 20 recommendations remain unimplemented. Two of the recommendations are Unresolved, which means that the FDIC has not provided an acceptable solution to resolve the recommendations. These recommendations include establishing and implementing a means to share classified information with Regional Offices, and ways

for Regional Offices to handle classified information once received.

In addition to ensuring the FDIC's receipt of relevant and actionable threat information, the FDIC should have assurances that banks obtain such threat information. We have work ongoing to determine whether the FDIC has implemented effective processes to ensure that FDIC-supervised and insured institutions receive actionable and relevant threat and vulnerability information.

Ensuring Adequate Data Collection and Analysis

The Government's Federal Data Strategy (FDS) promotes harnessing existing data; anticipating future uses of existing and potentially available data; and demonstrating responsiveness by improving data collection, analysis, and dissemination by seeking input from users and stakeholders. The FDS also highlights the critical importance of sharing data among Government agencies to inform decision-making and allow for thorough analyses.

The FDIC should have reliable data for decision-making at all levels of the Agency and to enable the FDIC Board to exercise its governance responsibilities. Further, the FDIC should have capabilities to analyze data to identify important trends. Incorrect, incomplete, and otherwise faulty data can lead to ineffective decision-making especially when data is the basis for policy determinations. Therefore, it is critical that the FDIC support and maintain data integrity.

In our recent OIG audits, evaluations, and reviews, we have found several examples of significant shortcomings in FDIC data, including:

- **Inadequate Use and Analysis of FDIC Data.** In our OIG review, Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program (January 2023), we found that the FDIC is not fully utilizing available tools and data to improve the effectiveness of the FDIC's IT examination program and to identify emerging risks at financial institutions. In 2017, the FDIC developed a tool to conduct analysis of unstructured data from IT examinations to improve IT examinations. However, the FDIC had not used the tool's analytics measures in the past 4 years (since 2018). In our OIG review, Sharing of Threat Information to Guide the Supervision of Financial Institutions (January 2022), we found that the FDIC was not performing trend analysis of data collected by FDIC examiners, such as those available in electronic documents and other supervisory records, nor had the FDIC established procedures to guide its data analysis. In our OIG report, The FDIC's Management of Employee Talent (September 2021), we found that the FDIC did not have a process for collecting and analyzing the various types of data that can be used to assess employee retention across the Agency as part of its talent management strategy. Specifically, the FDIC did not have a systematic process to holistically capture and analyze data, and to ensure that the information flowed to the FDIC Divisions and Offices.

- **Unreliable Data and Incorrect Reporting.** In four OIG reports, we found that FDIC data was unreliable, and in one report, unreliable data led to inaccurate reports to the FDIC Board of Directors.

    - In our OIG evaluation, Termination of Bank Secrecy Act/Anti-Money Laundering

Consent Orders (December 2021), we found that the FDIC did not consistently track Consent Order termination data in its system of record. As a result, the FDIC provided nine incorrect reports to the FDIC Board of Directors concerning enforcement actions; and did not report three BSA/AML Consent Order terminations in a quarterly report to FinCEN.

- In our OIG evaluation, The FDIC's Personnel Security and Suitability Program (January 2021), we found that contractor position risk levels recorded in FDIC systems were unreliable. As a result, the FDIC could not determine whether these contractors received background investigations commensurate with their positions. We also found that FDIC systems were missing data for employee and contractor preliminary background investigation completion dates.

- In our OIG audit, FDIC's Compliance under the Digital Accountability and Transparency Act of 2014 (November 2021), we found that the FDIC's submission of financial and award data excluded information for the Federal Savings and Loan Insurance Corporation Resolution Fund and the Resolution Trust Corporation.

- In our OIG evaluation, Reliability of Data in the FDIC Virtual Supervisory Information on the Net System (November 2021), we found that two of the four key data elements we tested in the FDIC's ViSION system, were not reliable. Errors in either date increase the risk of inaccurate reporting of examination performance metrics to FDIC management.

The FDIC has addressed the recommendations in these reports.

A key element to ensuring financial stability is the flow of timely and actionable threat information from across the Federal Government. Banks' receipt of threat information allows them to take mitigating action. Threat information also assists the FDIC in conducting bank examinations, implementing supervisory approaches, and making policy determinations. In addition, analysis of reliable and accurate FDIC program data facilitates measurement and assessment of FDIC programs by the FDIC Board and senior management.

Strengthening FDIC Contracting and Supply Chain Management

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Addressing continued weaknesses in FDIC contracting systems and processes;
- Managing the FDIC's supply chain; and
- Ensuring whistleblower rights and protections for contractor personnel.

The OIG has identified Contracting and Supply Chain Management as a Top Challenge for the FDIC since 2018.

The FDIC awards nearly $600 million in contracts every year. Over a 5-year period, the FDIC awarded more than 2,600 contracts valued at $2.85 billion. The FDIC procures goods and services, including for the continuity of its operations, IT systems support, legal services, and resolution and receivership activities. For its IT needs alone, the FDIC contracts for about $400 million per year, and the Agency has more than 3,700 contract employees. The FDIC should have an effective internal control environment and culture to ensure that its procurements are timely, cost-effective, and within the terms of the awards.

Goods and services should also be rendered to the FDIC through secure supply chains. The Federal Government has acknowledged the need for secure supply chains in order to maintain its economic strength and national security.[69] On November 16, 2022, CISA issued an alert that a Federal Executive Branch Agency's network was compromised through a software vulnerability.[70] In this instance, the threat actors exploited unpatched vulnerabilities in a server, were able to move laterally throughout the network, compromised credentials, and implanted mining and other software.

The FDIC also should ensure that its contract employees are able to report fraud, waste, abuse, and mismanagement at the Agency without fear of retaliation or reprisal, and that they are aware of their whistleblower rights and protections.

Addressing Continued Weaknesses in FDIC Contracting Systems and Processes

FDIC contracting efforts require significant improvement. The former FDIC Chairman recognized the urgent need for improvements in the area of contract oversight management. In June 2021, the former FDIC Chairman acknowledged that "[i]n the last 10 years, the [FDIC CIOO] has been the subject of 303 recommendations from the [OIG] or the GAO. Roughly 61 of these recommendations, or 20 percent, related to program management or acquisition issues. About 62 reflected inadequate policies, procedures or program documentation."[71] Further, the former FDIC Chairman stated that "[t]he FDIC acquisition process has also been routinely criticized during this period with [an] additional 55 contracting recommendations. ...[t]hey point to systemic cultural shortfalls that must be remedied."

In March 2021, the FDIC began moving its entire acquisition processes to a new procurement system known as the FDIC Acquisition Management System (FAMS). In June 2022, FAMS was deployed to all users. However, in September 2022, just 16 months later, the Agency decided to revert back to its earlier system known as the Automated Procurement System (APS) and reassess the use of FAMS. The FDIC installed FAMS at a cost of $7.6 million and more than 8,300 staff hours. In order for the FDIC to transition from FAMS back to APS,

Agency personnel needed to manually enter contracts into the old APS. We have work planned to assess the FAMS procurement.

Also, in our OIG evaluation, Contract Oversight Management (October 2019), we determined that the APS had limited data and reporting capabilities for Agency-wide oversight of its contract portfolio. We found that the FDIC was overseeing acquisitions on a contract-by-contract basis, rather than on a portfolio basis. Therefore, the FDIC 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 risks or plan for future acquisitions. We recommended that the FDIC provide enhanced contract portfolio reports to FDIC Executives, senior management, and the Board of Directors. This recommendation remains unimplemented since the issuance of the report more than 3 years ago.

For the past 2 years, the GAO has also identified significant deficiencies in the FDIC's internal controls over financial reporting related to FDIC contracting. In 2020, the GAO identified deficiencies in the FDIC's controls over contract payment review processes and stated that "the FDIC cannot reasonably assure internal controls over contract payments are operating effectively, which increases the risks of improper payments and financial statement misstatements."[72] In 2021, the GAO identified significant deficiencies in the FDIC's controls over contract payment review and documentation processes. The GAO noted that the deficiencies may have resulted in a "misstatement in unaudited financial information FDIC reported internally and externally."[73]

Further, in our OIG evaluation, Critical Functions in FDIC Contracts (March 2021), we found that the FDIC did not have policies and procedures to identify Critical Functions at the Agency, nor did it implement any heightened monitoring of these Critical Functions.[74] Therefore, the FDIC could not be assured that it would provide sufficient management oversight of contractors performing Critical Functions or supervision to ensure that the Agency did not lose control of its mission or operations. We made 13 recommendations to strengthen the FDIC's identification and monitoring of contracts involving Critical Functions, and as of the date of this Top Challenges Report, 12 recommendations remain unimplemented. We have additional work ongoing to assess other FDIC contracts.

Managing the FDIC's Supply Chain

According to NIST, organizations face risks that the products and services they acquire "may contain potentially malicious functionality, are counterfeit, or are vulnerable to poor manufacturing and development practices within the supply chain."[75] An agency may have reduced visibility, understanding, and control of these risks when its vendors rely on second- and third-tier suppliers and service providers. The GAO noted that Federal agencies face supply chain risks, "including threats posed by malicious actors who may exploit vulnerabilities in the supply chain, and, thus compromise the confidentiality, integrity, or availability of an organization's systems and the information they contain."[76]

Because the FDIC is a financial regulator and holds vast amounts of sensitive and nonpublic information, adversaries may seek to disrupt the Agency's operations, programs, and functions and may manipulate or exploit the sensitive information for their own purpose or benefit. As noted by NIST, "adversaries are using the supply chain as an attack vector and [as an] effective means of penetrating [United

States' public and private] systems, compromising the integrity of system elements, and gaining access to critical assets."[77]

In our OIG report, The FDIC's Implementation of Supply Chain Risk Management (March 2022), we examined whether the FDIC developed and implemented its SCRM Program in alignment with the Agency's objectives and best practices. We found that the FDIC was not conducting supply chain risk assessments in accordance with best practices. Specifically:

- The FDIC had not identified known risks to the FDIC's supply chain;
- The FDIC did not define a risk management framework to evaluate risks to non-IT procurements; and
- The FDIC had not established metrics and indicators related to continuous monitoring and evaluation of supply chain risks.

Absent SCRM implementation and risk assessments, supply chain risks could compromise FDIC IT and data and provide adversaries a means to exfiltrate sensitive information such as confidential bank examination information. Further, the FDIC's supply chain could compromise the products, services, and facilities that enable the FDIC to perform its mission.

We made nine recommendations to the FDIC to improve its SCRM program and ensure contract document retention. As of the date of this Top Challenges Report, six recommendations remain unimplemented, nearly a year after issuance of our report.

In our OIG report, the FDIC's Information Security Program—2022 (September 2022), we similarly found that the FDIC had not yet developed its policies and procedures to address SCRM.

Ensuring Whistleblower Rights and Protections for Contractor Personnel

In our OIG report, Whistleblower Rights and Protections for FDIC Contractors (January 2022), we found that the FDIC had not aligned its procedures and processes with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections. The FDIC also did not always comply with the requirements to notify contractors of their whistleblower rights and protections.

The FDIC's Legal Division did not adopt any whistleblower rights notification provisions for contractors or include any whistleblower clauses in its contracts. The FDIC also did not verify that contractors and subcontractors notified employees of their whistleblower rights and protections. We made nine recommendations to improve the FDIC's compliance with legal requirements for whistleblower contractor clauses. As of this Top Challenges Report, four recommendations remain unimplemented, more than a year after issuance of our report.

Contract and supply chain management are critical to the FDIC's mission. Absent an accountable organizational culture and effective internal controls, the FDIC may not have insight into the reliability and integrity of the supply chain for its procured goods and services. Further, absent whistleblower protections, contractors may not report waste, fraud, and abuse in FDIC contracts.

Implementing Effective Governance at the FDIC

Key Areas of Concern

The primary areas of concern for this Challenge are:

- Capturing the FDIC's enterprise risks;
- Addressing repeat and unimplemented recommendations in a timely manner;
- Using outcome measures of performance;
- Explaining whether the FDIC will follow Executive Branch guidance; and
- Ensuring the validity and efficacy of FDIC rulemaking.

The OIG has identified Governance as a Top Challenge at the FDIC since 2018.

The FDIC Board of Directors (FDIC Board) and senior officials are responsible for the governance of the FDIC.[78] Governance refers to a management framework that incorporates operational, financial, risk management, and reporting processes, so that FDIC Board members and senior officials can effectively plan, govern, and meet strategic objectives.[79] A governance framework should ensure strategic guidance, effective monitoring of management, and accountability to stakeholders.[80] Effective governance is critical to ensure that the FDIC assesses and addresses risks—especially those identified in this Report. Governance also should ensure consistent implementation of FDIC policies and effective rulemaking.

Capturing the FDIC's Enterprise Risks

An important role for the FDIC Board is oversight of the Agency's ERM program.[81] ERM is an essential component of governance that provides an entity-wide view of the full spectrum of internal and external risks facing an organization.

Effective ERM provides information to FDIC Board members and senior officials, so that they can allocate resources appropriately, effectively prioritize and proactively manage risk, improve the flow of risk information, and work towards achieving the FDIC's mission. Further, the FDIC should use its ERM process whenever it makes significant decisions or organizational changes affecting the enterprise. Absent robust identification, assessment, and mitigation of these risks, and the use of ERM in FDIC decision-making, the FDIC may be hindered in its ability to achieve its mission.

In our OIG evaluation, The FDIC's Implementation of Enterprise Risk Management (July 2020), we determined that ERM was not fully implemented at the FDIC, and, therefore, proper execution of program activities, roles, and responsibilities had yet to take place. In recent OIG reports issued since that time, we continue to find that the FDIC has not considered or captured important internal and external risks into its ERM processes. For example:

> **Contracting**. In our OIG report Critical Functions in FDIC Contracts (March 2021), we found that the FDIC's Risk Inventory did not recognize procured Critical Functions as a separate and distinct risk, or as an analytical factor in determining inherent or residual risk associated with cybersecurity and privacy support services. As a result, the FDIC relied heavily on a contractor to mitigate controls for potential FDIC cyber-attacks and/or data breach losses.
>
> **Climate-related Financial Risk**. In our Top Challenges Report for 2021,

we noted that the FDIC's ERM program had not fully considered the financial risks associated with climate change as identified in the FSOC Climate Report. Absent identification of climate-related risk within the ERM program, the FDIC budget, staff, and efforts did not focus on identifying and addressing related risks. In November 2022, the FDIC added climate-related risks to its ERM program.

Operations in a Continuing Hybrid Work Environment. The FDIC has not identified risks for its hybrid work model. Beginning in September 2022, 80 percent of FDIC staff chose a home-based work option, meaning their home has become their primary place of work. The FDIC has not assessed how its new hybrid environment may impact the FDIC's crisis readiness.

Sharing of Threat Information. In our OIG report, Sharing of Threat Information to Guide the Supervision of Financial Institutions (January 2022), we found that the FDIC did not establish effective processes to acquire, analyze, disseminate, and use relevant and actionable threat information to guide the supervision of financial institutions. The FDIC had not included threat sharing as an ERM risk.

Addressing Repeat and Unimplemented Recommendations in a Timely Manner

The FDIC Board and senior officials should ensure that program weaknesses are promptly resolved and remediated in a timely manner. If recommendations are not addressed expeditiously, the FDIC faces an increased likelihood that the underlying vulnerabilities or deficiencies will continue or recur until remediated by the FDIC. Therefore, the FDIC should prioritize the corrective actions intended to address the recommended improvements, in line with the timing and representations made by the Agency at the time of our reports, and it should allocate sufficient resources to implement such corrective actions.

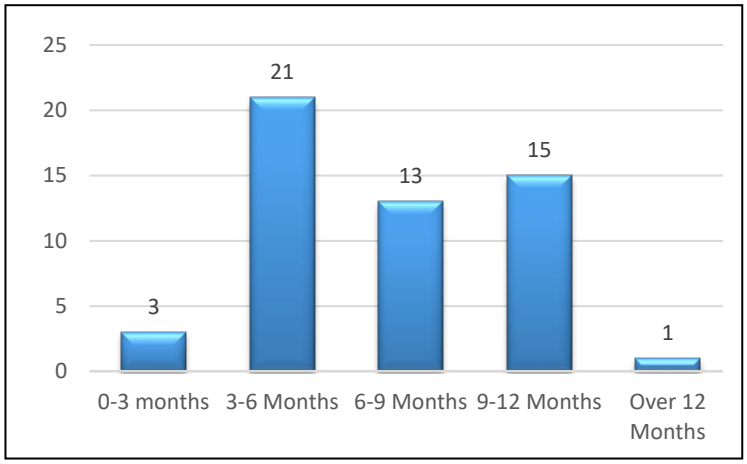
The OIG has made repeated recommendations for several programs and processes at the FDIC, including:

- **Cybersecurity Vulnerabilities.** In each of our past five annual OIG reviews of FDIC Information Security (2018 through 2022), we reported weaknesses related to the FDIC's management of Administrative Accounts. Weaknesses in the FDIC's processes for managing Administrative Accounts increase the risk of unauthorized activity, such as individuals accessing, modifying, deleting, or exfiltrating sensitive information. We also found that the FDIC has not taken timely action or has not addressed POA&Ms, which is a management tool used by the Agency to track the progress of corrective actions pertaining to security vulnerabilities identified through security control assessments and other sources. Without consistently addressing control deficiencies in a timely manner, FDIC data is vulnerable to security exploits from unmitigated threats.

- **Weaknesses in the FDIC's Personnel Security and Suitability Program.** In our OIG evaluation, The FDIC's Personnel Security and Suitability Program (PSSP) (January 2021), we found several deficiencies that were similar to those identified in previous reports—including our OIG evaluation of the FDIC's PSSP conducted 6 years earlier in 2014. Specifically, a number of issues had not been corrected, including: Completing preliminary background investigations within allowed timeframes; Keeping records of background investigation documentation; Ensuring that background investigation levels match an individual's position risk; and Ensuring the reliability of background investigation data in FDIC systems. Similarly, in our OIG Management Advisory Memorandum, Background Investigations for Privileged Account Holders (June 6, 2022), we identified that the FDIC did not have adequate controls to ensure that certain contractors and employees who require privileged access to FDIC information systems and data had background investigations commensurate with their positions. As a result, the FDIC could not be sure that certain employees and contractors who were granted privileged access to the FDIC's information systems and related data subsequent to their onboarding would have an appropriate risk designation level and related background investigations.

Further, for 73 percent of the outstanding OIG report recommendations (53 of 73 recommendations), the FDIC amended its initial corrective action completion dates several times. At the time of the issuance of an OIG report, the FDIC sets the timeframe to implement changes to address OIG recommendations. In general, it takes the FDIC an average of 8 months to take corrective action. However, when the FDIC extends its implementation timeframe, the weaknesses that we identified continue to persist. As shown in Figure 9, the FDIC amended its implementation dates by moving them from 3 to more than 12 months beyond the FDIC's initial implementation dates.

Figure 9: FDIC Extension of Corrective Action Dates



Source: OIG analysis of corrective action dates and extensions.

Using Outcome Measures of Performance

The GPRA Modernization Act of 2010 requires that agencies measure program performance. Further, according to the GAO, "[p]erformance measures may address the direct products and services delivered by a program (outputs), or the results of those products and services (outcomes)." The GAO noted that "agencies should make every attempt to identify and use outcome goals whenever possible to reflect the results of their activities."[82] The key to outcome-oriented performance measures is that they allow an agency to assess whether it is meeting a program's strategic objectives.

We found instances where the FDIC either did not have program performance measures in place, or used output rather than outcome measures to assess program

performance. As a result, the FDIC cannot assess whether its programs are achieving the desired outcomes. For example, in our report Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program (January 2023), we found that the FDIC established goals focused on improving the FDIC's supervision program, but did not have a way to measure the outcome of this goal. Without establishing metrics for the FDIC's IT examinations, the FDIC is unable to determine whether its IT examination activities under the InTREx Program are achieving their desired outcomes or results.

The GAO's report, Banking Services: Regulators Have Taken Actions to Increase Access, but Measurement of Actions' Effectiveness Could be Improved (February 2022), found that the FDIC lacked outcome-oriented measures to assess FDIC efforts to increase banking access for unbanked and underbanked individuals. For example, the GAO stated, the "FDIC piloted a public awareness campaign on the benefits of bank accounts. Yet, its measures indicate only whether a task was completed and do not incorporate information on the outcomes (which could be used to assess the activities)."

Also, in our OIG Memorandum, The FDIC's Management of Employee Talent (September 2021), we found that the FDIC had not established metrics or indicators to measure the effectiveness of its retention activities or actions for examination staff. Instead, the FDIC tracked its "inputs" – that is, the implementation status of the activities or actions designed to meet its employee retention goals. The FDIC did not measure whether its activities were achieving their desired outcomes or results. Thus, the FDIC could not determine whether its retention activities were working effectively nor how to make improvements to its processes.

Explaining Whether the FDIC Will Follow Executive Branch Guidance

The Executive Branch regularly issues guidance for Federal agencies, in the form of Executive Orders, Presidential Directives, Office of Management and Budget (OMB) Circulars and Memoranda, and NIST guidance. Such guidance often addresses risks in operational areas, such as information technology, security, privacy, contracting, and risk management. The policies and guidance provide best practices that Executive Branch agencies should implement to mitigate operational risks.

The FDIC makes policy decisions to sometimes follow such requirements, and other times not. It is not clear under what circumstances and which specific portions or provisions of the policies or guidance are to be followed. Ambiguity in the FDIC's determinations and lack of clarity may result in inconsistencies with other agencies (including other bank regulators) and may cause uncertainty and confusion among FDIC employees in the application of such policies and guidance. For example, in our OIG report, Whistleblower Rights and Protections for FDIC Contractors (January 2022), we found that the FDIC's DOA Acquisition Services Branch voluntarily adopted some of the Federal whistleblower provisions and requirements for insertion into its contracts. However, the FDIC's Legal Division, under its separately delegated contracting authority, did not operate consistently with the FDIC's DOA. The FDIC Legal Division had neither adopted any whistleblower rights notification provisions for contractors nor included any whistleblower clauses in its contracts. We also found that FDIC procedures and processes were not aligned with laws, regulations, and policies designed to ensure notice to contractor and subcontractor employees about their whistleblower rights and protections.

Further, in our recent OIG reports, we found that when the FDIC did not implement Executive Branch guidance regarding administration, management, and governance, its programs incurred risks that these policies were intended and designed to address or mitigate:

- **Contracting:** The OMB issued Policy Letter 11-01 to provide Federal agencies with guidance on managing contracts for the performance of Critical Functions.[83] The FDIC's Legal Division concluded that the Policy Letter did not apply to the FDIC, but it may be used for guidance. In our OIG evaluation, Critical Functions in FDIC Contracts (March 2021), we found that the FDIC did not have policies and procedures for identifying Critical Functions in its contracts, as recommended by the OMB Policy Letter. Without these practices, the FDIC could not be assured that it will provide sufficient management oversight of contractors performing Critical Functions.

- **Enterprise Risk Management:** In 2016, in an effort to modernize existing agency risk management efforts across the Federal Government, the OMB updated its Circular A-123.[84] The FDIC took the position that it was not required to follow OMB Circular A-123. As noted earlier, in our OIG evaluation, The FDIC's Implementation of Enterprise Risk Management (July 2020), we found that the FDIC did not fully implement its ERM program in accordance with OMB criteria. Specifically, the FDIC did not establish a clear governance structure, and clearly define authorities, roles, and responsibilities related to ERM. Further, the FDIC did not clearly define the roles, responsibilities, and processes of the committees and groups involved in ERM.

- **Rulemaking Cost Benefit Analysis:** In our report, Cost Benefit Analysis Process for Rulemaking (February 2020), we found that the FDIC did not follow identified best practices from Executive Orders, the GAO, and other Federal agencies to establish and document a process for determining when to perform cost benefit analyses and how the analyses should be conducted. We made five recommendations to improve the FDIC's cost benefit analyses. The FDIC has implemented all five recommendations.

The FDIC should clearly articulate and explain its determinations regarding whether or not to follow Executive Branch policies and guidance, and it should be transparent under what circumstances and which specific portions or provisions of the policies or guidance are to be followed. Consistent analysis and application, and documentation of these decisions would enhance public confidence and transparency of FDIC operations, programs, and functions.

Ensuring the Validity and Efficacy of FDIC Rulemaking

On October 19, 2022, the U.S. Court of Appeals for the Fifth Circuit ruled that the funding of the Bureau of Consumer Financial Protection (CFPB) violated the appropriations clause of the Constitution and, as a result, the CFPB's Payday Lending Rule was invalid.[85] The CFPB receives it funding from the Federal Reserve, which is funded through bank assessments. The Court explained that this funding structure is not subject to the Congressional appropriations process and therefore violated the Appropriations

Clause. There is a risk that the Fifth Circuit's ruling could also be applied to the FDIC. The FDIC is funded outside of the Congressional appropriations process through bank assessments (similar to the Federal Reserve).

Also, FDIC rulemaking should be a transparent process that analyzes the need for bank regulation and the compliance burden placed on banks. A foundational component of transparent rulemaking is the FDIC's access to reliable information to measure a regulation's costs and benefits.

Effective governance is critical to ensure proper oversight of the FDIC and the accomplishment of its mission. The FDIC Board and management should ensure that the FDIC is identifying and managing risks through an effective ERM program and promptly addressing recommendations made by the OIG and GAO to address identified risks. The FDIC should measure program effectiveness by establishing outcome measurements and also address whether the FDIC will follow Executive Branch guidance. The FDIC should ensure the validity of its rulemaking and ensure that rules are premised on solid cost benefit analyses.

---

[1] Board of Governors of the Federal Reserve, *Financial Stability Report* (May 2022).
[2] FSOC, *Report on Digital Asset Financial Stability Risks and Regulation* (2022); FSOC, *Report on Climate-Related Financial Risk* (2021); FSOC *Annual Report 2022*.
[3] European Central Bank Working Paper Series, *A Wake-up Call Theory of Contagion* (May 2022).
[4] OECD, *Financial Markets and Climate Transition, Opportunities, Challenges and Policy Implications* (April 10, 2021).
[5] Rainforest Action Network, *Banking on Climate Chaos, Fossil Fuel Finance Report 2022* (March 30, 2022).
[6] Journal of Finance, *Did FinTech Lender Facilitate PPP Fraud?* (August 18 2021, revised August 17, 2022).
[7] According to the Government Accountability Office, "[t]he Dodd-Frank Act does not use the term 'systemically important financial institution (SIFI).' This term is commonly used by academics and other experts to refer to bank holding companies with $50 billion or more in total consolidated assets and nonbank financial companies designated by the Financial Stability Oversight Council." GAO, *Bank Regulation: Lessons Learned and a Framework for Monitoring Emerging Risks and Regulatory Response* (June 2015).
[8] 12 USC § 5326. Bear Sterns and AIG received loans through the Federal Reserve Bank of New York, but Lehman Brothers did not receive loans.
[9] Notice and request for comment, Federal Register, *Resolution of Systemically Important Financial Institutions: The Single Point of Entry Strategy* 78 Fed. Reg. 76,614 (December 18, 2013); Notice extension of comment period, Federal Register, *Resolution of a Systemically Important Financial Institution: The Single Point of Entry Strategy* 79 Fed. Reg. 9,899 (February 21, 2014).
[10] In 2013, the OIG reviewed FDIC OLA planning efforts. In our report, *The FDIC's Progress in Implementing Systemic Resolution Authorities* (November 2013), we found that more work needed to be done by the FDIC to establish an FDIC-wide capability to implement systemic resolutions under the Dodd-Frank Act. As a result, we made six recommendations aimed at enhancing the FDIC's long-term strategic planning efforts, strengthening coordination among FDIC Divisions, and building out the Office of Complex Financial Institution's infrastructure to support systemic resolution activities. The FDIC provided a plan for future actions to implement these recommendations. The OIG closed the recommendations based on the FDIC's plans for future actions and stated that the OIG would continue to monitor the FDIC progress. In 2017, the OIG revised its process and now reviews all corrective actions to determine whether the FDIC's actions satisfy the recommendation before the recommendation is considered closed.
[11] The Financial Stability Board (FSB) has designated the following U.S.-based companies as "global systemically important banks": Bank of America, Bank of New York Mellon, Citigroup, Goldman Sachs, JP Morgan Chase, Morgan Stanley, State Street Corporation, and Wells Fargo. The FSB is an international body that monitors and makes recommendations about the global financial system. The FSB publishes annually a list of GSIBs using calendar year-end data and an assessment methodology designed by the Basel Committee on Banking Supervision (BCBS). The FSB, consulting with BCBS and national authorities, has identified GSIBs since 2011.
[12] Foreign GSIBs that have systemically important operations in the United States include: Barclays, Credit Suisse, Deutsche Bank, HSBC, and UBS.
[13] Financial Market Utilities are multilateral systems that provide infrastructure for transferring, clearing, and settling payments, securities, and other financial transactions among financial institutions or between financial institutions and the clearing/settlement system. 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. 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.

[14] The Dodd-Frank Act created the Council of Inspectors General on Financial Oversight (CIGFO) to oversee the activities of the Financial Stability Oversight Council. CIGFO is chaired by the Inspector General of the Department of the Treasury and its membership includes the Inspectors General of the Board of Governors of the Federal Reserve System, Commodity Futures Trading Commission, Department of Housing and Urban Development, Federal Deposit Insurance Corporation, Federal Housing Finance Agency, National Credit Union Administration, Securities and Exchange Commission, and Special Inspector General for the Troubled Asset Relief Program.

[15] Statement of Martin J. Gruenberg, Acting Chairman, FDIC, before the United States Senate, Committee on Banking, Housing, and Urban Affairs, *Oversight of Financial Regulators: A Strong Banking System for Main Street* (November 15, 2022).

[16] OCC Bulletin 2021-34, *Small Business Administration Lending: Risk Management Principles* (August 5, 2021). Additional risks include: **Operational risk:** A financial institution that does not have staff with the requisite knowledge of Government-guaranteed loan program requirements may realize losses due to its inability to operate within the Government-guaranteed loan program requirements. **Compliance risk:** A financial institution that does not comply with the Government-guaranteed loan program requirements could face civil money penalties or restitution. **Liquidity Risk**: Financial institutions can sell Government-guaranteed loans in the secondary market at a premium, which increases liquidity. **Reputation risk:** A financial institution that haphazardly engages in Government-guaranteed loan programs can result in negative public opinion or costly litigation. **Strategic risk:** A financial institution that makes a strategic decision to only originate Government-guaranteed loans may realize reduced revenue, resulting in operating losses if a Federal agency suspends its ability to originate Government-guaranteed loans.

[17] Congress of the United States, House of Representatives, Select Committee on the Coronavirus Crisis, Staff Report, *"We Are Not The Fraud Police": How Fintechs Facilitated Fraud In The Paycheck Protection Program* (December 2022).

[18] Department of Commerce, International Trade Administration, *Russia – Country Commercial Guide, Sanctions Framework* (July 21, 2022).

[19] FinCEN, *FinCEN Advises Increased Vigilance for Potential Russian Sanctions Evasion Attempts* (March 7, 2022).

[20] Verizon data showed that the financial industry accounted for 690 data breaches (13 percent) of the 5,212 data breaches reviewed in 2021.

[21] VMWare, *Modern Bank Heist 5.0* (April 2022).

[22] Fitch Ratings, *Exploratory Research: Quantifying U.S. Bank Systemic Cybersecurity Risk* (August 10, 2021).

[23] American Banker, *Small New York bank reports data breach* (March 14, 2022).

[24] Remarks by Acting Comptroller of the Currency Michael J. Hsu before the Joint Meeting of the Financial and Banking Information Infrastructure Committee and the Financial Services Sector Coordinating Council (August 2, 2022).

[25] OCC Semiannual Risk Perspective Spring 2022.

[26] VMWARE, *Modern Bank Heist 5.0* (April 20, 2022). Island hopping refers to infiltrating a bank through its vendor relationships that are also known as its third parties.

[27] VMWare, *Modern Bank Heist 5.0* (April 2022).

[28] See *Proposed Interagency Guidance on Third-Party Relationships: Risk Management*, 86 Fed. Reg. 38,182 (September 17, 2021).

[29] Final Rule, *Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers*, 86 Fed. Reg. 66,424 (November 23, 2021).

[30] 12 C.F.R. § 304.22(b)(7).

[31] The 41 banks include banks supervised by the FDIC and other regulators.

[32] ViSION is the FDIC's **V**irtual **S**upervisory **I**nformation **O**n the **N**et.

[33] Cointelegraph, *Total Crypto Market Cap Falls to $840 billion, but Derivatives Data Show Traders are Neutral* (December 8, 2022).

[34] The Washington Post, *These Banks Were Left Holding the Bag in Crypto Implosion* (November 23, 2022).

[35] Wall Street Journal, *Silvergate Raced to Cover $8.1 Billion in Withdrawals During Crypto Meltdown* (January 5, 2023); Wolf Street, *Crypto-Bank Silvergate Details its Own Implosion, Much of its Equity Capital Wiped Out, I'm waiting for the FDIC to Show Up* (January 5, 2023).

[36] American Banker, *What the Indictments Against FTX's Sam Bankman-Fried Means for Banks* (December 28, 2022); Forbes, *Why Did FTX Buy Into a U.S. Bank Owned by a Co-Creator of 'Inspector Gadget'* (December 2, 2022).

[37] Basel Committee on Banking Supervision, *Discussion Paper: Designing a Prudential Treatment for Crypto-assets* (May 2021).

[38] FinCEN, *Advisory on Illicit Activity Involving Convertible Virtual Currency* (May 9, 2019).
[39] Federal Trade Commission, *Reported Crypto Scam Losses Since 2021 Top $1 Billion, Says DTC Data Spotlight* (June 3, 2022).
[40] Reuters, *Cryptocurrency and Anti-money laundering Enforcement* (September 26, 2022).
[41] The Department of Justice has noted the importance of training and retaining investigators and prosecutors to handle changing and complex digital asset-related matters such as money laundering. See Department of Justice, *The Role of Law Enforcement In Detecting, Investigating, and Prosecuting Criminal Activity Related to Digital Assets* (September 2022).
[42] Final Rule, *False Advertising, Misrepresentation of Insured Status, and Misuse of the FDIC's Name or Logo* (June 2, 2022).
[43] FDIC Press Release, *FDIC and Federal Reserve Issue Letter Demanding Voyager Digital Cease and Desist from Making False or Misleading Representations of Deposit Insurance Status* (July 28, 2022).
[44]Forbes, *Binance.US Is Not Buying Voyager's Crypto Assets for $1.02 Billion. Here's What Really Happening* (December 19, 2022). Bloomberg, *Voyager Customers With Frozen Savings on "Edge of Seat" Ahead of Auction* (September 12, 2022); CNBC, *Voyager Customer Lost $1 Million Saved Over 24 Years And Is One Of the Many Now Desperate To Recoup Funds* (August 15, 2022).
[45] *Joint Letter Regarding Potential Violations of Section 18(a)(4) of the Federal Deposit Insurance Act* (July 28, 2022).
[46] Financial Institution Letter 35-2022, *Advisory to FDIC-Insured Institutions Regarding Deposit Insurance and Dealings with Crypto Companies* (July 29, 2022).
[47] FDIC Press Release, *FDIC Issues Cease and Desist Letters to Five Companies For Making Crypto-Related False or Misleading Representations about Deposit Insurance* (August 19, 2022).
[48] The World Bank, *Financial Inclusion*.
[49] Federal Reserve Board FED Notes, *Wealth Inequality and the Racial Wealth Gap* (October 22, 2021).
[50] The FDIC's Economic Inclusion Strategic Plan is intended to promote the widespread use of affordable and sustainable products and services from insured depository institutions that help consumers meet their financial goals.
[51] GAO, *Banking Services: Regulators Have Taken Actions to Increase Access, but Measurement of Actions' Effectiveness Could Be Improved* (February 2022).
[52] The *Blueprint for an AI Bill of Rights* is intended to support the development of policies and practices that protect civil rights and promote democratic values in the building, deployment, and governance of automated systems. However the Blueprint is non-binding and does not constitute U.S. Policy.
[53] Federal Register, *Request for Information and Comment on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning*, 86 Fed. Reg.16,837 (March 31, 2021).
[54] CISA, *Binding Operational Directive 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 3, 2021).
[55] GAO, *High Risk Area: Ensuring Cybersecurity of the Nation*.
[56] Executive Office of the President of the United States, *Federal Information Security Modernization Act of 2014 Annual Report to Congress Fiscal Year 2021*.
[57] CISA Alert (AA-22-320A) *Iranian Government-Sponsored Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvest* (November 16, 2022).
[58] CISA, *Binding Operational Directive 22-01-Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 3, 2021).
[59] 12 C.F.R. Parts 309, 310.
[60] GAO Snapshot, *Cloud Computing: Federal Agencies Face Four Challenges* (September 2022).
[61] FDIC Directive 2120.1, *Personnel Security and Suitability Program for Applicants and Employees* (updated January 15, 2020).
[62] GAO, *Privacy: Federal Financial Regulators Should Take Additional Actions to Enhance Their Protection of Personal Information* (January 2022).
[63] FedWeek, *Federal workforce attrition rises back up to pre-pandemic levels* (August 3, 2022).
[64] GAO, *Cybersecurity: Bank and Other Depository Regulators Need Better Data Analytics and Depository Institutions Want More Usable Threat Information* (July 2015), Figure 7 notes Federal sources of cyber threat information relevant to banks. Examples of Federal threat information include: The Financial and Banking Information Infrastructure Committee chartered under the President's Working Group on Financial Markets shares non-public cyber threat information pertaining to financial institutions. The Treasury Department and its component organizations: The Office of Cybersecurity and Critical Infrastructure Protection shares information about cybersecurity and physical threats and vulnerabilities; the Office of Intelligence and Analysis (OIA) has responsibility for the receipt, analysis, collation, and dissemination of foreign intelligence and foreign counterintelligence information related to the operation; FinCEN collects and analyzes financial transaction information provided by financial institutions; OFAC publishes lists of individuals and companies owned or controlled by, or acting for or on behalf of, countries subject to sanctions. OFAC also lists individuals, groups, and entities, such as terrorists and narcotics traffickers. The Department of Homeland Security provides analysis, expertise, and technical assistance to critical infrastructure owners and operators, and conducts vulnerability assessments. The FBI also disseminates information regarding specific threats to entities, including insured financial institutions through various methods, including Private Industry Notifications and Liaison Alert System reports.
[65] See FSOC *2022 Annual Report* and the OCC *Semiannual Risk Perspective* (Spring 2022).

[66] NIST, Special Publication 800-150, *Guide to Cyber Threat Information Sharing* (October 2016).
[67] GAO Issue Summary, *Using Data and Evidence to Improve Federal Programs*. Forbes, *How The U.S. Federal Government Is Mobilizing To Enable Data-Driven Decision Making* (June 1, 2022).
[68] See CISA critical infrastructure definition.
[69] Executive Order 13806, *Assessing and Strengthening the Manufacturing and Defense Industrial Base and Supply Chain Resiliency of the United States* (July 21, 2017), emphasizes that resilient supply chains are essential to the economic strength and national security of the U.S.; Executive Order 14017, *Executive Order on America's Supply Chains* (February 24, 2021), states that the U.S. needs resilient, diverse, and secure supply chains to ensure our economic prosperity and national security; and Executive Order 14028, *Improving the Nation's Cybersecurity* (May 17, 2021), includes actions to enhance software supply chain security.
[70] CISA Alert (AA-22-320A) *Iranian Government-Sponsored Actors Compromise Federal Network, Deploy Crypto Miner, Credential Harvest* (November 16, 2022).
[71] *Minutes of the Meeting of the Board of Directors – Federal Deposit Insurance Corporation* (June 2021).
[72] GAO, *Management Report: Improvements Needed in FDIC's Internal Control over Contract-Payment Review Processes* (May 13, 2021).
[73] GAO, *Management Report: Improvements Needed in FDIC's Internal Control over Contract-Payment Review Processes* (May 19, 2022).
[74] OMB Policy Letter 11-01, *Performance of Inherently Governmental and Critical Functions* (February 13, 2012), defined a Critical Function as "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."
[75] NIST SP 800-161r1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations* (May 2022).
[76] GAO, *Cybersecurity: Federal Agencies Need to Implement Recommendations to Manage Supply Chain Risks* (May 25, 2021).
[77] NIST Special Publication 800-37, *Risk Management Framework for Information Systems and Organizations: A System LifeCycle Approach for Security and Privacy* (December 2018)
[78] The FDIC Board has five members who are appointed by the President and confirmed by the Senate. Board members include: the FDIC Chairman, FDIC Vice Chairman, Comptroller of the Currency, Director of the Bureau of Consumer Financial Protection (CFPB), and an independent Director. The FDIC Board has designated the FDIC Operating Committee as the "focal point" for the coordination of risk management at the FDIC.
[79] Deloitte, *Developing an effective governance operating model – A guide for financial services boards and management teams*.
[80] Organization for Economic Co-operation and Development (OECD), *G20/OECD Principles of Corporate Governance* (2015).
[81] 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).
[82] GAO, *Banking Services: Regulators Have Taken Actions to Increase Access, but Measurement of Actions' Effectiveness Could be Improved* (February 2022).
[83] OMB Office of Federal Procurement Policy, Policy Letter 11–01, *Performance of Inherently Governmental and Critical Functions* (February, 13, 2012).
[84] OMB Circular No. A-123, *Management's Responsibility for Enterprise Risk Management and Internal Control* (July 15, 2016).
[85] *Community Financial Services of America v. Consumer Financial Protection Bureau* (October 19, 2022).

Federal Deposit Insurance Corporation
Office of Inspector General

3501 Fairfax Drive
Room VS-E-9068
Arlington, VA 22226

(703) 562-2035

★★★★★★

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in FDIC programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding FDIC programs, employees, contractors, or contracts, please contact us via our Hotline or call 1-800-964-FDIC.