2024 Report on Cybersecurity and Resilience

FDIC

FEDERAL DEPOSIT INSURANCE CORPORATION

Table of Contents –

Executive Summary

The Federal Deposit Insurance Corporation (FDIC) submits this report on cybersecurity and resilience to the Committee on Financial Services of the House of Representatives and the Senate Committee on Banking, Housing, and Urban Affairs pursuant to Section 108 of the Consolidated Appropriations Act, 2021.

The FDIC is the primary federal regulator of federally insured, state-chartered depository institutions that are not members of the Federal Reserve System (referred to in this report as "FDIC-supervised financial institutions");[1] serves as the nation's deposit insurer; acts as receiver for insured depository institutions that fail; and has resolution planning responsibilities (jointly with the Board of Governors of the Federal Reserve System) for large and complex financial companies.

The report first discusses how the FDIC maintains and strengthens its own cybersecurity. The FDIC protects its systems, the sensitive personal and business information it has related to its own operations, and sensitive information it has related to the operations of banks and service providers. The FDIC pursues its own cybersecurity initiatives, achieves government-wide goals, and complies with applicable federal law and regulation to continuously improve its cybersecurity posture. Independent audits of the FDIC's compliance with the Federal Information Security Modernization Act of 2014[2] (FISMA) provide additional information to focus FDIC cybersecurity efforts.

The report next discusses FDIC actions to strengthen cybersecurity in the financial services sector. The FDIC promulgates rules, in coordination with other bank regulators or alone, and enforces those rules and applicable laws that promote cybersecurity and resilience through the supervision and examination of FDIC-supervised financial institutions and by examining services provided by certain service providers. More specifically, the FDIC evaluates financial institutions' cybersecurity practices for safety and soundness; shares information and provides technical assistance through guidance, alerts, and advisories; communicates via in-person and virtual meetings with financial institutions and service providers on cybersecurity matters; hires and trains examiners and cybersecurity analysts; maintains examination work programs and other resources; and conducts information technology examinations. The FDIC also collaborates on cybersecurity matters with other state and federal banking regulators, law enforcement, intelligence, and security agencies, and the private sector. Additionally, the FDIC uses information from independent audits to improve the effectiveness and management of its supervisory programs.

The fight against malicious actors who use cyberspace to harm others requires constant vigilance and agility. The FDIC will continue to collaborate with stakeholders to maintain a resilient financial system in spite of the evolving cybersecurity threat.

[1] The FDIC has primary supervisory authority over insured state nonmember banks, state-licensed insured branches of foreign banks that are subject to the provisions of section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831), and state savings associations.
[2] 113th United States Congress, *Federal Information Security Modernization Act of 2014*, Public Law 113-283, December 18, 2014, https://www.congress.gov/113/plaws/publ283/PLAW-113publ283.pdf.

FDIC Cybersecurity

This section discusses how the FDIC maintains and strengthens its own cybersecurity. It first describes the FDIC's policies and procedures relevant to cybersecurity and resilience, and then discusses how the FDIC implements those policies and procedures, including the FDIC's efforts to respond to Office of Inspector General (OIG) recommendations, Executive Order (EO) 14028,[3] the Office of Management and Budget (OMB) Memoranda, and Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) cybersecurity directives.

Policies and Procedures

The FDIC collects and maintains a variety of information, including, for example, employee information and bank-related information (such as reports of examination) that may contain business sensitive data (confidential supervisory information), or sensitive personally identifiable information (PII). The FDIC has an important responsibility to protect this information. The FDIC information security program provides standards, policies, best practices, and architecture oversight to the FDIC information systems, business processes, and outsourced services. The program is consistent with relevant federal requirements and guidelines, including FISMA requirements, OMB policy, DHS CISA guidance, and the National Institute of Standards and Technology (NIST) security standards and guidelines. Of note, FDIC Directive 1310.3, *Information Security Risk Management Program*, defines the FDIC's Information Security Risk Management Program responsibilities with respect to the management of risk to data and to the information systems and services that use the data in compliance with FISMA and NIST Special Publication (SP) 800-37.[4]

In 2023, FDIC updated key policies and procedures impacting essential security and privacy control areas to align with federal policies, guidance, and standards; and further codified key roles and responsibilities into the FDIC's Information Systems Security Management Program. The FDIC established policies, including FDIC Directive 1360.16, *Mandatory Cybersecurity and Privacy Awareness Training* (April 2023) which require all FDIC employees and contractor personnel with network access to complete the Cybersecurity and Privacy Awareness Training (CPAT). In addition, Directive 1360. 09, *Protecting Information* (July 2023) provides policy on the rules of behavior for protecting information created, collected, and maintained by the FDIC with rules of behavior and effective security practices; and requirements governing the FDIC's collection, use, sharing, and protection of information according to its sensitivity. Key areas of focus in 2023 included: 1) updating and maintaining the security and privacy controls catalog with FDIC defined parameters and supplemental guidance, 2) enhancing the FDIC implementation of the CISA Continuous Diagnostics and Mitigation (CDM) Program, and 3) maturing the Assessment and Authorization process for contractor-managed information systems.

In addition, the FDIC continues to adopt a corporate-wide risk-based approach to the delivery of information technology (IT) services and risk management by defining its corporate-wide risk management strategy, risk appetite, and risk tolerance levels. In the OIG report entitled *The*

[3] EO 14028, *Improving the Nation's Cybersecurity*, May 12, 2021, https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.
[4] NIST, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, December 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

FDIC's Information Security Program – 2023,[5] the auditors concluded "the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines." The overall FDIC Information Security Program maturity rating for 2023 was Level 4 (*Managed and Measurable*),[6] indicating that the information security program is operating at an effective level of security. However, the auditors also concluded that there were "security control weaknesses [that] continue to pose risk to the FDIC." In its response, FDIC management concurred with two recommendations related to process improvements associated with the removal of user network accounts and technical issues preventing enforcement of security and privacy training compliance. In addition, the FDIC closed six out of the nine recommendations from prior-year FISMA audits and it is working to complete the necessary corrective actions to close the three remaining unimplemented recommendations from the 2021 and 2023 FISMA Audit reports.

Implementation

The FDIC has an established information security program that continues to progress and evolve to meet new challenges. Recently, the FDIC completed certain actions to strengthen its security controls such as implementing an enterprise-wide Document Labeling Program to support data protection and privacy related controls, and completing its efforts to apply the NIST Risk Management Framework (RMF) to all systems and applications.

The FDIC continues to maintain and improve information security consistent with EOs and guidance issued by OMB, DHS CISA, and NIST. For example, the FDIC has:

- Accelerated the implementation of a cloud infrastructure solution to enhance the resiliency, security, and scalability of the FDIC's Mission Essential/Mission Critical (ME/MC) systems and deployed four ME/MC business systems as part of this cloud solution;
- Continued efforts toward a Zero Trust Architecture (ZTA) in accordance with EO 14028 and aligned with the CISA Zero Trust Maturity Model;
- Made steady progress with refinements and improvements to the FDIC's information security and privacy continuous monitoring program;
- Enhanced cyber risk management processes for third-party systems;
- Implemented a new incident management solution to enhance existing capabilities related to the timely detection, response, and recovery from cybersecurity incidents and data breaches;
- Migrated the FDIC enterprise logging and Security Information and Event Management (SIEM) platforms to the cloud for enhanced incident detection and response capabilities;

[5] FDIC Office of Inspector General, *The FDIC's Information Security Program – 2023*, September 2023, https://www.fdicoig.gov/sites/default/files/reports/2023-12/AUD-23-004-Redacted.pdf.
[6] CIGIE, *FY 2023 IG FISMA Metrics Evaluator's Guide*, April 27, 2023, https://www.cisa.gov/sites/default/files/2023-05/fy_2023_ig_fisma_metrics_evaluation_guide.pdf.

- Continued to mature the cyber threat intelligence program for improved threat monitoring, threat hunting and modeling capabilities;
- Enhanced the process for collecting and assessing vulnerability disclosures from security researchers by adopting CISA's Vulnerability Disclosure Policy (VDP) Platform; and
- Implemented process improvements to ensure confidentiality agreements for contractor and subcontractor personnel are properly executed and maintained.

Despite this progress, there are areas where the FDIC is focusing its attention on improvements. For example, the FDIC continues its efforts in the areas of management of End-of-Life and End-of-Service software, aging Plans of Action and Milestones, privileged account management, and security training compliance. The FDIC will continue to focus its efforts on maturing controls in these areas.

The FDIC's Security Response Team (SRT) provides centralized technical assistance to effectively investigate and resolve security incidents involving FDIC information. There were 616 security events reported to the SRT from October 1, 2022 through September 30, 2023. These security events involved U.S.-based systems and generally had limited impact. None of these events met the criteria for classification as a Major incident. During the same period, the FDIC reported 133 of these incidents to the United States Computer Emergency Readiness Team (US-CERT) following the US-CERT Federal Incident Notification Guidelines.[7] All of the incidents reported to US-CERT received a CISA National Cyber Incident Scoring System (NCISS) priority score of either Baseline – Negligible or Baseline – Minor.

The EO 14028 on *Improving the Nation's Cybersecurity*[8] outlines several cybersecurity measures and requirements intended to harden our nation's digital infrastructure against increasingly frequent and sophisticated cyberattacks.

- Remove Barriers to Threat Information sharing between government and the private sector. The EO ensures that IT Service Providers are able to share information with the government and requires them to share certain breach information.
- Modernize and implement stronger Cybersecurity Standards in the Federal Government. The EO promotes movement of the Federal Government to secure cloud services and a zero-trust architecture, and mandates the development of multi-factor authentication (MFA) and data encryption (at-rest and in-transit) within a specific time period. Additionally, OMB issued Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,*[9] that set a federal zero trust architecture strategy, and requires agencies to meet specific cybersecurity standards and objectives by the end of FY 2024 in order to reinforce the Government's defenses against increasingly sophisticated and persistent threat campaigns. The FDIC has responded to all the required actions.

[7] CISA, *US-CERT Federal Incident Notification Guidelines*, https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.
[8] White House, *Executive Order on Improving the Nation's Cybersecurity*, May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.
[9] OMB, M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles*, January 26, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

- Improve Software Supply Chain Security. The EO improves the security of software by requiring the Secretary of Commerce and others to establish baseline security standards for development of software sold to the government, including requiring developers to maintain greater visibility into software and making security data publicly available. It also creates a pilot consumer labeling program so that one can quickly determine whether software was developed securely. OMB issued Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices,*[10] and followed with M-23-16, *Update to Memorandum M-22-18 Enhancing Software Supply Chain through Secure Software Development Practices*[11], directing executive departments and agencies to comply with the NIST guidance, which provides recommendations on ensuring that the producers of software an agency procures have been following a risk-based approach for secure software development. The FDIC is working to respond to all the required actions.
- Improve Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Networks. The EO improves the ability of agencies to detect malicious cyber activity on federal networks by requiring a government-wide endpoint detection and response (EDR) system and improved information sharing within the Federal Government. OMB issued Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems Through Endpoint Detection and Response*,[12] directing the Federal Government to adopt a robust EDR solution as part of the shift in cyber defense from a reactive to a proactive posture. The M-22-01 memorandum provides implementation guidance to agencies to accelerate the adoption of EDR solutions and improve visibility into and detection of cybersecurity vulnerabilities and threats to the Government, as defined in EO 14028. The FDIC has responded to all the required actions.
- Improve the Federal Government's Investigative and Remediation Capabilities. The EO creates cybersecurity event log requirements for federal departments and agencies to improve their ability to detect intrusions, mitigate those in progress, and determine the extent of an incident after the fact. OMB issued Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*,[13] to address the requirements of the EO for logging, log retention, and log management with a focus on supporting centralized access and visibility for the highest-level enterprise security operations center (SOC) of each agency. In addition, this memorandum establishes requirements for agencies to increase the sharing of such information, as needed and appropriate, to accelerate incident response efforts and to enable more effective defense of federal information

[10] OMB, M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, September 14, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.
[11] OMB, M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, June 9, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security-1.pdf.
[12] OMB, M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response*, October 8, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.
[13] OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-31-Improving-the-Federal-Governments-Investigative-and-Remediation-Capabilities-Related-to-Cybersecurity-Incidents.pdf.

and Executive Branch departments and agencies. CISA published *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities*[14] to provide additional information to aid agencies in prioritizing the implementation of the policy requirements outlined in M-21-31. The FDIC has updated its control catalog so new systems will meet the M-21-31 requirements, and is assessing requirements for legacy systems.

Furthermore, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*,[15] to provide reporting guidance and deadlines in accordance with FISMA 2014 and to ensure agencies are continuing to drive forward the implementation of EO 14028. The memorandum is designed to modernize FISMA data collection in five key ways:

- Measuring zero trust implementation: Agencies are required to take discrete, time-bound steps by FY 2024 to meet the goals of EO 14028 and M-22-09.
- Clear, actionable, and outcome-focused data: M-22-05[16] initiated significant changes in the Government's approach to FISMA oversight and CIO and Inspector General (IG) metrics collection. This memorandum builds upon those advancements and will ultimately provide the Executive Office of the President, Congress, and the public with a clear view of agencies' security achievements and challenges. To ensure agencies can continue to focus on outcomes over manual reporting, the FY 2023 CIO metrics will fully automate certain reporting.
- Ensuring input from across the Federal enterprise: This guidance also establishes a CISO Council FISMA Metrics Subcommittee tasked with advising OMB on refining and improving FISMA guidance and metrics.
- Improving security-privacy coordination: While independent and separate disciplines, security and privacy also have a close relationship per OMB Circular A-130, *Managing Information as a Strategic Resource*.[17] Coordination across these disciplines is essential to managing security and privacy risks and to complying with applicable requirements as outlined in this memorandum.
- Improving incident response: This memorandum builds on Administration efforts to ensure CISA works closely with Federal agencies in building a cohesive, coordinated incident response infrastructure. EO 14028 laid out a series of actions to modernize the Federal Government's investigative and remediation capabilities.

The FDIC reported the FY 2023 quarterly and annual FISMA CIO metrics to track the implementation of NIST standards, as well as other cybersecurity-related initiatives, including those in support of EO 14028.

[14] CISA, *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities*, December 2022, https://www.cisa.gov/sites/default/files/2023-02/TLP%20CLEAR%20-%20Guidance%20for%20Implementing%20M-21-31_Improving%20the%20Federal%20Governments%20Investigative%20and%20Remediation%20Capabilities.pdf.
[15] OMB, OMB, M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, December 2, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/12/M-23-03-FY23-FISMA-Guidance-2.pdf.
[16] OMB, M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf.
[17] OMB, OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

Additionally, OMB issued the following Memoranda in which the FDIC is in compliance where applicable:

- Memorandum M-23-10, *The Registration and Use of .gov Domains in the Federal Government,*[18] directs all Federal agencies on the acceptable use and registration of Internet domain names as required by the DOTGOV Online Trust in Government Act of 2020.[19] The FDIC has responded to all the required actions.
- Memorandum M-23-13, *"No TikTok on Government Devices" Implementation Guidance*,[20] directs all Federal agencies to remove and disallow installations of the TikTok application on IT owned or operated by agencies, or use by contractors. The FDIC has responded to all the required actions.
- Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*,[21] aligns with EO 14028 as it focuses on the security and integrity of the software supply chain and emphasizes the importance of secure software development environments. This memorandum reaffirms the importance of secure software development practices and extends the timelines for agencies to collect attestations from software producers. Additionally, this memorandum provides supplemental guidance on the scope of M-22-18[22] requirements and on agencies' use of Plan of Actions and Milestones (POA&Ms) when software producer cannot provide the required attestation, but plans to do so. The FDIC is working to respond to all the required actions.
- Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence*, directs all agencies to advance artificial intelligence (AI) governance and innovation while managing risks from the use of AI in the Federal Government, particularly those affecting the rights and safety of the public. The FDIC is working to respond to all the required actions.

Additionally, FISMA authorizes DHS, in coordination with OMB, to develop and oversee the implementation of cybersecurity Binding Operational Directives (BODs) and Emergency Directives (EDs), outlining activities that require federal agency compliance. BODs address agency implementation of OMB policies, principles, standards, and guidelines. EDs address known or reasonably suspected information security threats, vulnerabilities, and incidents that represent a substantial threat to agencies. CISA leads the DHS efforts to develop, communicate, and manage actions and critical activities related to all directives, in close coordination with OMB.

[18] OMB, M-23-10, *The Registration and Use of .gov Domains in the Federal Government*, February 8, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-10-DOTGOV-Act-Guidance.pdf.
[19] United States 116th Congress, *Consolidated Appropriations Act, 2021*, Pub. L. No. 116-260, §§ 901-07, December 27, 2020, https://www.congress.gov/116/plaws/publ260/PLAW-116publ260.pdf.
[20] OMB, M-23-13, *"No TikTok on Government Devices" Implementation Guidance*, February 27, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/02/M-23-13-No-TikTok-on-Government-Devices-Implementation-Guidance_final.pdf.
[21] OMB, M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, June 9, 2023, https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf.
[22] OMB, M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*, September 14, 2022, https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.

The FDIC fully complied with the two BODs and two EDs from FY 2023 into FY 2024 issued by CISA:

- ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities:[23] CISA observed widespread and active exploitation of vulnerabilities in Ivanti Connect Secure and Ivanti Policy Secure solutions. Successful exploitation of the vulnerabilities in these affected products allows a malicious threat actor to move laterally, perform data exfiltration, and establish persistent system access, resulting in full compromise of target information systems. CISA has determined these conditions pose an unacceptable risk to Federal Civilian Executive Branch (FCEB) agencies and require emergency action. The FDIC completed all required actions.
- CISA issued Supplemental Direction V1: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities:[24] The Supplemental Direction V1 supersedes the required action 4 in ED 24-01 which is applicable to all Federal agency running affected products (Ivanti Connect Secure or Ivanti Policy Secure solutions). Threat actors continue to leverage the vulnerabilities to capture credentials and drop webshells that enable further compromise of the enterprise networks. Some threat actors have recently developed workarounds to earlier mitigations and detection methods and have been able to exploit weaknesses, move laterally, and escalate privileges without detection. CISA is aware of instances in which threat actors have minimized traces of their intrusion, limiting the effectiveness of the external integrity checker tool (ICT). The FDIC completed all required actions.
- CISA issued a second Supplemental Direction V2: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities:[25] The Supplemental Direction V2 supersedes Supplemental Direction V1 and Required Action 4 in ED 24-01 for any federal agency running Ivanti Connect Secure or Ivanti Policy Secure solutions. Ivanti reported a new vulnerability affecting a limited number of supported Ivanti Connect Secure and Ivanti Policy Secure solutions. This newly disclosed vulnerability enables an attacker to access restricted resources without authentication. Ivanti released new security updates that replaced previous updates released on January 31 and February 1, 2024. CISA is aware of instances in which threat actors have minimized traces of their intrusion, limiting the effectiveness of the external integrity checker tool (ICT). The FDIC completed all required actions.
- ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System:[26] The Russian state-sponsored cyber actor known as Midnight Blizzard has exfiltrated email correspondences between FCEB agencies and Microsoft through a successful compromise of Microsoft corporate email accounts. Microsoft has disclosed the incident and follow on updates through multiple communications,

[23] CISA, ED 24-01, *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*, January 19, 2024, https://www.cisa.gov/news-events/directives/ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure-vulnerabilities.
[24] CISA, Supplemental Direction V1: ED 24-01, *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*, January 31, 2024, https://www.cisa.gov/news-events/directives/supplemental-direction-v1-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure.
[25] CISA, Supplemental Direction V2: ED 24-01, *Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*, February 9, 2024, https://www.cisa.gov/news-events/directives/supplemental-direction-v2-ed-24-01-mitigate-ivanti-connect-secure-and-ivanti-policy-secure.
[26] CISA, ED 24-02, *Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*, April 2, 2024, https://www.cisa.gov/news-events/directives/ed-24-02-mitigating-significant-risk-nation-state-compromise-microsoft-corporate-email-system.

beginning in January 2024: *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*[27] and *Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*[28]. Midnight Blizzard's successful compromise of Microsoft corporate email accounts and the exfiltration of correspondence between agencies and Microsoft presents a grave and unacceptable risk to agencies. CISA requires agencies to analyze the content of exfiltrated email, reset compromised credentials, and take additional steps to ensure authentication tools for privileged Microsoft Azure accounts are secure. Microsoft and CISA have notified all federal agencies whose email correspondence with Microsoft was identified as exfiltrated by Midnight Blizzard. The FDIC has completed all required actions and continues to coordinate with CISA as new information concerning this event is discovered.

- BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks:[29] Continuous and comprehensive asset visibility is a basic pre-condition for any organization to effectively manage cybersecurity risk. Accurate and up-to-date accounting of assets residing on federal networks is also critical for CISA to effectively manage cybersecurity for the FCEB enterprise. The requirements of this Directive focus on two core activities essential to improving operational visibility for a successful cybersecurity program: asset discovery and vulnerability enumeration. The goal of this Directive is for agencies to comprehensively achieve outcomes such as: maintain an up-to-date inventory of networked assets as defined in the scope of this Directive; identify software vulnerabilities using privileged or client-based means where technically feasible; track how often the agency enumerates its assets, what coverage of its assets it achieves, and how current its vulnerability signatures are; and provide asset and vulnerability information to CISA's Continuous Diagnostic and Mitigation (CDM) Federal Dashboard. These requirements advance the priorities set forth in the EO 14028 Section 7 (*Improving Detection of Cybersecurity Vulnerabilities and Incidents of Federal Government Networks*), and provide operational clarity in achieving policy set forth in previous OMB Memoranda, including M-21-02[30], M-22-05, and M-22-09. Compliance with this Directive also supports BOD 22-01, *Managing Unacceptable Risk Vulnerabilities in Federal Enterprise*, as it will enable agencies to enhance the management of known exploited vulnerabilities that can be detected using automated tools. The FDIC completed all required actions.
- BOD 23-02: Mitigating the Risk from Internet-Exposed Management Interfaces:[31] As agencies and organizations have gained better visibility of their networks and improved endpoint detection and response, threat actors have adjusted tactics to evade these protections by targeting network devices supporting the underlying network infrastructure. Recent threat campaigns underscore the grave risk to the federal

[27] Microsoft, *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*, January 19, 2024, https://msrc.microsoft.com/blog/2024/01/microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/.
[28] Microsoft, *Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*, March 8, 2024, https://msrc.microsoft.com/blog/2024/03/update-on-microsoft-actions-following-attack-by-nation-state-actor-midnight-blizzard/.
[29] CISA, BOD 23-01, *Improving Asset Visibility and Vulnerability Detection on Federal Networks*, October 3, 2022, https://www.cisa.gov/news-events/directives/binding-operational-directive-23-01.
[30] OMB, M-21-02, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*, November 9, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/11/M-21-02.pdf.
[31] CISA, BOD 23-02, *Mitigating the Risk from Internet-Exposed Management Interfaces*, June 13, 2023, https://www.cisa.gov/news-events/directives/binding-operational-directive-23-02.

enterprise posed by improperly configured network devices. Inadequate security, misconfiguration, and out of date software make these devices more vulnerable to exploitation. The risk is further compounded if device management interfaces are connected directly to, and accessible from, the public-facing internet. Most device management interfaces are designed to be accessed from dedicated physical interfaces and/or management networks and are not meant to be accessible directly from the public internet. CISA requires agencies to take steps to reduce the attack surface created by insecure or misconfigured management interfaces across certain classes of devices. The FDIC completed all required actions.

FDIC Controls: Over the past year, there continued to be a significant number of high-profile ransomware attacks against corporations, state and local government entities, and non-profits. The organizations affected often experienced reputational damage, significant remediation costs, and interruptions in the delivery of core services. The number and impact of publicly reported ransomware events has made ransomware a significant factor in today's cybersecurity landscape. NIST Cybersecurity Framework v 2[32] identifies three core technical capabilities (NIST calls these "functions") that are most relevant to attacks such as ransomware: Protect, Detect, and Recover.

The FDIC has implemented and maintains a number of layered and complementary controls to counter the threat of ransomware and other forms of malware. Among these controls are: phishing assessments that simulate real-world phishing emails; automated tools to scan email and block known malicious domains; network segmentation to protect the most valuable IT assets; strong filters to prevent phishing emails from reaching end-users; egress filtering on servers to restrict outbound Internet connections; tools supporting auditing, log collection, log analysis, and log correlation; an updated incident response plan; and senior management exercises to practice incident response.

Financial Services Sector Cybersecurity

This section discusses FDIC actions to strengthen cybersecurity in the financial services sector and highlights policies and procedures relevant to cybersecurity and resilience. This section also discusses how the FDIC reviews financial institutions' implementation of risk management programs consistent with these FDIC policies to address cyber-risks.

Policies and Procedures

The FDIC publishes safety and soundness rules, standards, guidance, and other information to assist FDIC-supervised financial institutions and their service providers with establishing effective risk management programs to address cybersecurity risks. The FDIC and the other federal banking agencies make most of these resources available on the FDIC and Federal

[32] NIST, *The NIST Cybersecurity Framework (CSF) 2.0*, February 26, 2024, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

Financial Institutions Examination Council (FFIEC)[33] websites[34] for reference by financial institutions and other entities, and periodically update these resources.

Safety and Soundness Standards

Section 39 of the Federal Deposit Insurance Act (12 U.S.C. 1831) requires the FDIC to establish safety and soundness standards for FDIC-supervised financial institutions that provide the framework for FDIC examinations. Under Section 39, the FDIC has issued the Interagency Guidelines Establishing Standards for Safety and Soundness, which are set forth as Appendix A to Part 364 of the FDIC's Rules and Regulations.

Appendix B to Part 364 contains Interagency Guidelines Establishing Information Security Standards. The FDIC issued these Guidelines under Section 39 of the Federal Deposit Insurance Act and Sections 501 and 505(b) of the Gramm-Leach-Bliley Act.[35] These Guidelines set forth standards for financial institutions regarding administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information. These information security standards provide the foundation for cybersecurity programs on which a financial institution can build controls effective for the unique risks it faces.

Computer-Security Incident Notification Rule

Effective May 1, 2022,[36] banking organizations, including FDIC-supervised financial institutions, must notify their primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after determining that such an incident has occurred. Timely notification of significant computer-security incidents allows federal banking regulators to have early awareness of emerging threats to banking organizations and the broader financial system. The Computer-Security Incident Notification rule requires notification to the federal banking regulators for incidents that have materially affected—or are reasonably likely to materially affect—the viability of a banking organization's operations, its ability to deliver banking products and services, or the stability of the financial sector. The rule also requires a bank service provider to notify its affected banking organization customers as soon as possible when the provider determines that it has experienced a computer-security incident that has materially affected or is reasonably likely to materially affect the provision of covered services to its banking organization customers for four or more hours.

As a principal member of the Cyber Incident Reporting Council (CIRC),[37] formed in response to the Cyber Incident Reporting for Critical Infrastructure Act of 2022

[33] The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the Board of Governors of the Federal Reserve System, the FDIC, the National Credit Union Administration (NCUA), the OCC, and the Consumer Financial Protection Bureau, and to make recommendations to promote uniformity in the supervision of financial institutions.

[34] Periodically, the federal banking agencies, the NCUA, and representatives of state agencies that supervise financial institutions send information to institutions and service providers via non-public channels.

[35] 15 U.S.C. 6801, 6805(b).

[36] FDIC, Financial Institution Letter No. FIL-74-2021, *Computer-Security Incident Notification Final Rule*, November 18, 2021, https://www.fdic.gov/news/financial-institution-letters/2021/fil21074.html.

[37] 6 U.S.C. § 681f.

(CIRCIA),[38] the FDIC is working with CISA and other regulatory agencies on a multi-year initiative to improve the Federal Government's visibility into cyber threats. This work seeks to harmonize Federal incident reporting requirements for U.S. financial institutions and other covered entities to avoid conflicting, duplicative, or burdensome requirements. During 2023, the FDIC and the other CIRC agencies provided input to DHS's report to Congress entitled "Harmonization of Cyber Incident Reporting to the Federal Government."[39] This DHS report includes: (1) a review of Federal cyber incident reporting requirements; (2) a discussion of the challenges to achieve harmonization; (3) proposed actions for DHS; and (4) potential legislation that may be needed to address duplicative reporting. During 2023 and 2024, the FDIC also consulted on a CISA notice of proposed rulemaking, published in April 2024, which requests public comment on key cyber incident definitions and reporting thresholds.[40]

Guidance

The FDIC publishes cybersecurity guidance unilaterally and jointly with other regulators. The FDIC typically coordinates development of guidance through the FFIEC. In some cases, the FDIC issues guidance independently or in collaboration with the Board of Governors of the Federal Reserve System (FRB) and the Office of the Comptroller of the Currency (OCC). Examples of recent cyber-risk guidance include:

- On May 3, 2024, the FDIC, FRB, and OCC released a guide titled, *Third-Party Risk Management - A Guide for Community Banks,* to support community banks in managing risks presented by third-party relationships.[41] The guide offers potential considerations, resources, and examples through each stage of a third-party relationship. A number of the considerations and resources in the guide relate to information security and cybersecurity in the context of third-party relationships.
- In June 2023, the FDIC, FRB, and OCC issued joint guidance[42] to financial institutions regarding the management of risks associated with third-party relationships. This joint guidance sets forth principles for risk management to assist financial institutions in overseeing their third-party relationships, including consideration of information security and operational risk associated with such relationships. The guidance highlights that risk management practices at an individual financial institution can be tailored consistent with the level of risk, the complexity and size of the financial institution, and the nature of the third-party relationship.

[38] *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law No. 117-103 Division Y.
[39] DHS, *Harmonization of Cyber Incident Reporting to the Federal Government* (September 2023). https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government.
[40] DHS, Proposed Rule, *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements* (April 4, 2024). https://www.federalregister.gov/documents/2024/04/04/2024-06526/cyber-incident-reporting-for-critical-infrastructure-act-circia-reporting-requirements.
[41] FDIC, Press Release, *Agencies Issue Guide to Assist Community Banks to Develop and Implement Third-Party Risk Management Practices* (May 3, 2024) https://www.fdic.gov/news/press-releases/agencies-issue-guide-assist-community-banks-develop-and-implement-third-party.
[42] FDIC, Financial Institution Letter No. FIL-29-2023, *Interagency Guidance on Third-Party Relationships: Risk Management,* June 6, 2023, https://www.fdic.gov/news/financial-institution-letters/2023/fil23029.html.

- In August 2021, the FFIEC member entities published guidance on Authentication and Access to Financial Institution Services and Systems,[43] which sets forth examples of risk management principles and practices for effective authentication of financial institutions' customers, employees, and other users. Effective authentication of customers, employees, and other users into the financial institution's information technology systems is a key control to mitigate a range of security threats, including ransomware.

Alerts and Advisories

In 2014, the FDIC recommended, through the FFIEC, that financial institutions of all sizes participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC) as part of their processes to identify, respond to, and mitigate cybersecurity threats and vulnerabilities.[44] This recommendation has been highlighted in subsequent communications. The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate the public and private sectors' sharing of physical and cybersecurity threat and vulnerability information. The FS-ISAC is an example of a central source from which a financial institution or a service provider could obtain threat information originating from multiple government and private sector sources.

The FDIC believes that threat and vulnerability information from the FS-ISAC and other sources is important to help organizations inform their defensive activities and remediate system weaknesses. Internally, FDIC supervisory staff consider a variety of threat and vulnerability information sources including Suspicious Activity Reports,[45] bank incident notifications, examination findings, federal law enforcement and intelligence agency reports, and data from other non-governmental entities. In 2022, the FDIC formalized procedures for determining when the agency will communicate about threats and vulnerabilities to FDIC-supervised financial institutions, examined service providers, and FDIC employees. For example, in 2023 the FDIC, along with other federal banking agencies, shared risk information and remediation resources from CISA about the MOVEit file transfer application vulnerability and threats with all FDIC-insured financial institutions.

The FDIC, along with other federal and state regulators, communicated with financial institutions through non-public channels the following significant alerts and advisories since January 2023:

- FFIEC members' cybersecurity alerts regarding the MOVEit transfer file transfer application vulnerability, including a discussion of potential risks of cyberattacks affecting supervised institutions' third-party relationships and recommendations to remediate these risks (June 6, 2023 and September 18, 2023).

[43] FDIC, Financial Institution Letter No. FIL-55-2021, *Authentication and Access to Financial Institution Services and Systems*, August 11, 2021, https://www.fdic.gov/news/financial-institution-letters/2021/fil21055.html.
[44] FFIEC, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*, November 3, 2014, https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf.
[45] See 12 CFR 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve); 12 CFR 353 (FDIC); 12 CFR 748.1(c) (NCUA); 12 CFR 21.11 and 12 CFR 163.180 (OCC); and 31 CFR Chapter X (FinCEN).

- CISA and National Security Agency (NSA) advisory regarding the People's Republic of China State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure advisory (February 29, 2024).
- CISA, NSA, and other governmental agencies' advisory regarding the Joint Guidance on Identifying and Mitigating Living Off the Land Techniques (February 29, 2024).

Technical Assistance

The FDIC offers a variety of technical assistance to educate and assist staff and directors of FDIC-insured financial institutions. This technical assistance includes, but is not limited to, technical assistance videos,[46] a Directors' Resource Center portal, director/banker colleges, teleconferences and webinars, Community Bank Resource Kits, regional compliance newsletters, and individual assistance to institutions. FDIC technical assistance on the topics of cybersecurity and resilience since January 2022 has included:

- Ransomware Program for Small- to Mid-Sized Financial Institutions. The FDIC collaborated with the Financial and Banking Information Infrastructure Committee[47] (FBIIC) to host a virtual forum on ransomware risk and mitigation strategies for small- to mid-sized financial institutions (March 1, 2022).
- Computer-Security Incident Notification "Ask the Regulators" Forum. The FDIC, FRB, and OCC held a webinar for all FDIC-insured financial institutions and service providers to address industry questions about computer-security incident reporting (April 28, 2022).
- Preparing for Post-Quantum Cryptography. The FDIC collaborated with CISA through the FFIEC to provide all FDIC-insured financial institutions the opportunity to participate in a non-public virtual forum to discuss developments in quantum information science. Content addressed the potential to drive innovation across the economy, while highlighting the potential risk to the economic and national security of the United States (September 23, 2022).
- Cybersecurity Awareness instructional videos. The FDIC produced a technical assistance video that provides background information on cybersecurity and emphasizes the board's role in overseeing their bank's cybersecurity efforts. Additionally, the FDIC released a video that emphasizes the important role bank officers have in designing and maintaining information security programs in a dynamic and evolving cyber threat environment (November 30, 2023).

Additional notable cybersecurity- and resilience-related advisories and technical assistance resources for financial institutions issued over the past four years include:

[46] FDIC, *Directors' Resource Center Technical Assistance Video Program*, https://www.fdic.gov/regulations/resources/director/technical/cybersecurity.html.
[47] The FBIIC was chartered under the President's Working Group on Financial Markets and consists of 18 member organizations from across the federal and state financial services regulatory community. More information available at: www.fbiic.gov.

- The FDIC issued a *Joint Statement on Heightened Cybersecurity Risk*[48] in coordination with the OCC to remind supervised financial institutions of sound cybersecurity management principles (January 16, 2020).
- The FFIEC member agencies released a *Statement on Risk Management for Cloud Computing Services*.[49] The statement highlighted examples of risk management practices for a financial institution's safe and sound use of cloud computing services and safeguards to protect consumers' sensitive information from risks that pose potential consumer harm (April 30, 2020).
- The FDIC, along with the OCC and the FRB, released a joint statement titled *Sound Practices to Strengthen Operational Resilience*,[50] outlining sound practices designed to help large banks increase operational resilience. Examples of risks to operational resilience include cyberattacks, natural disasters, and pandemics (October 30, 2020).
- The FDIC jointly published an update to the FFIEC *Cybersecurity Resources Guide for Financial Institutions*[51] that provides a variety of free or low-cost cybersecurity-related resources. The updated resource guide now includes ransomware-specific resources (October 27, 2022).
- The FDIC, FRB, and OCC issued a joint statement on crypto-asset risks to banking organizations.[52] Among the key risks it highlights are heightened risks associated with open, public, or decentralized networks or similar systems, including risks from vulnerabilities related to cyber-attacks. Banking organizations are neither prohibited or discouraged from providing banking services to customers of any specific class or type, as permitted by law or regulation (January 3, 2023).
- The FDIC contributed views and perspectives to Treasury in connection with its report titled, *Financial Services Sector's Adoption of Cloud Services.*[53] This report reflects input from a broad outreach initiative with financial institutions of all sizes, cloud service providers, and industry trade associations. The Treasury report describes how adoption of public cloud services has increased rapidly over the last decade and that financial institutions of all sizes face an increasingly complex threat and technology environment as they expand their use of cloud services. Recommendations and next steps outlined in the report include cloud service provider tabletop exercises with the financial sector; consideration of operational and cybersecurity threats; policy development relating to system-wide measurement of concentration; and continued

[48] FDIC, Financial Institution Letter No. FIL-03-2020, *Joint Statement on Heightened Cybersecurity Risk,* January 16, 2020, https://www.fdic.gov/news/financial-institution-letters/2020/fil20003a.pdf.
[49] FFIEC, *FFIEC Issues Statement on Risk Management for Cloud Computing Services*, April 30, 2020, https://www.ffiec.gov/press/pr043020.htm.
[50] FDIC Press Release, *Agencies Release Paper on Operational Resilience*, October 30, 2020, www.fdic.gov/news/press-releases/2020/pr20122.html.
[51] FFIEC, *Cybersecurity Resources Guide for Financial Institutions*, November 2022, https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf.
[52] FDIC, *Agencies Issue Joint Statement on Crypto-Asset Risks to Banking Organizations*, January 3, 2023, https://www.fdic.gov/news/press-releases/2023/pr23002.html.
[53] U.S. Treasury, *The Financial Services Sector's Adoption of Cloud Services,* February 8, 2023, https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.

engagement internationally through standard setting bodies. (February 8, 2023). Following the issuance of this report, Treasury established the Cloud Services Steering Group (CSSG) to encourage and support collaboration among U.S. financial regulators, financial sector participants, and cloud service providers on integrity and resilience issues associated with the financial sector's use of cloud-based services. The work of the CSSG started in 2023, and will continue through 2024. FDIC staff is contributing to a number of work streams of the CSSG.

Outreach and Other Publications

The FDIC also periodically highlights to financial institutions information on the state of cybersecurity, particular threats and vulnerabilities, and effective controls to mitigate the related risks. Examples of this outreach during 2022 and 2023 include:

- *Treasury Unclassified Threat Exchanges.* Beginning in June 2022, the FDIC partnered with the U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) offering OCCIP briefings to FDIC-insured institutions. These virtual briefings are typically held monthly to share information on existing and emerging cybersecurity threats. These meetings are closed to the public and invitations are distributed monthly to FDIC-insured financial institutions through the FDIC's secure messaging system. These briefings are Traffic Light Protocol: AMBER,[54] meaning recipients may only share information with members of their own organization, and with clients or customers who need to know the information to protect themselves or prevent further harm (throughout 2022 and 2023).
- *Minority Depository and Community Development Institutions Outreach*. As part of the FDIC's commitment to Minority Depository and Community Development Institutions), the FDIC provided cybersecurity and IT technical assistance to institutions that provide banking services to minority and low- and moderate-income communities. Consultation topics in 2023 included: notification of engaging in crypto-related activities; Interagency Information Security Standards; cybersecurity preparedness; responding to IT examination matters (e.g., IT governance and business continuity planning); IT patch management; and IT risk assessments. In addition, regional outreach programs included discussions on IT due diligence, cybersecurity controls, and other IT-related topics.
- *2023 Risk Review*. The FDIC 2023 Risk Review provides financial institutions and the public an overview of banking conditions for 2022 through early 2023. The Risk Review's discussion of operational risk addresses the potential negative impact to banks from cyber threats and illicit activity (August 14, 2023).
- *Ransomware Webinar*. The FDIC, along with other banking sector regulators and the support of the Federal Bureau of Investigation (FBI), hosted an industry outreach webinar to provide updates on recent ransomware attack trends,

[54] Cybersecurity and Infrastructure Security Agency, *Traffic Light Protocol 2.0 User Guide*, September 2022, https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf.

including new data destruction tactics and mitigation recommendations (October 31, 2023).

- *Ask the Regulators Webinar: Third-Party Risk Management*. The FDIC, along with the OCC and FRB, offered a webinar to industry on the recently updated supervisory guidance for third-party risk management (July 26, 2023).
- *FDIC and Financial Crimes Enforcement Network (FinCEN) Digital Identity Tech Sprint.*[55] The FDIC in collaboration with FinCEN hosted a "tech sprint" focused on measuring the effectiveness of processes to collect, validate, and verify information to onboard customers. Innovation, consistent with cybersecurity controls and anti-money laundering requirements, was a focus of the Tech Sprint (April 2022).
- *FFIEC Multifactor Authentication Webinar*. The FDIC in partnership with the FFIEC and FinCEN hosted a non-public industry outreach webinar to discuss the importance of multifactor authentication as a critical control to support a layered authentication framework (November 18, 2022).
- *FDIC Directors' College and Regional Risk Conferences.*[56] The FDIC organizes course offerings for directors and officers. These programs offer timely and relevant cybersecurity and resiliency information and are often delivered in cooperation with state banking departments and industry trade groups (throughout 2022 and 2023).

Implementation

The FDIC examines IT risk management practices, including cybersecurity, at each FDIC-supervised financial institution as part of the risk management examination. The focus of these FDIC examinations relative to cybersecurity risk is on the safe and sound operation of the institution's IT systems. Based on the examination, examiners assign an IT rating to the financial institution using the FFIEC Uniform Rating System for Information Technology.[57] Examiners also incorporate the IT rating into the management component of the CAMELS rating.[58] During 2023, the FDIC conducted 1,243 IT examinations at FDIC-supervised institutions and service providers.

Each IT examination's results are documented in a written examination report that the FDIC provides to management of the financial institution. This examination report will detail any weakness in cyber practices at the financial institution that are identified during the IT examination. The FDIC may use informal and formal enforcement actions[59] to address weak operating practices identified during the examination.

[55] FDIC Press Release, *FDIC and FinCEN Launch Digital Identity Tech Sprint*, April 5, 2022, https://www.fdic.gov/news/press-releases/2022/pr22030.html.
[56] FDIC, Directors College Program, https://www.fdic.gov/resources/bankers/directors-college-program/index.html.
[57] FFIEC, *Supervision of Technology Service Providers (Appendix A)*, October 2012, https://www.ffiec.gov/press/pr103112.html.
[58] FDIC, RMS Manual of Examination Policies – Basic Examination Concepts and Guideline, March 2022 https://www.fdic.gov/regulations/safety/manual/section1-1.pdf.
[59] FDIC, *FDIC Formal and Informal Enforcement Actions Manual*, https://www.fdic.gov/regulations/examinations/enforcement-actions/index.html.

Separately, the FDIC's Division of Depositor and Consumer Protection examines FDIC-supervised financial institutions for compliance with privacy-related consumer protection laws and regulations.

Additionally, the FDIC's Division of Complex Institution Supervision and Resolution also participates in cybersecurity examinations at FDIC-insured financial institutions with assets greater than $100 billion where the FDIC is not the primary federal regulator, including the eight U.S. global systemically important banks. These examinations are conducted jointly with the OCC and FRB.

The Bank Service Company Act gives the FDIC authority to regulate and examine the performance of bank services provided to FDIC-supervised financial institutions. The FDIC frequently examines the performance of such services jointly with the FRB and OCC. States also join these examinations when there is overlapping authority and interest. Starting in 2021, bank service provider examinations include a review of service provider controls designed to defend against advanced cyber threats using cybersecurity examination procedures developed by the FDIC, FRB, and OCC to promote consistent evaluation of this risk.

FDIC staff, along with staff of the other federal banking agencies, also conduct periodic horizontal examinations, focusing on particular control or threat issues, of the certain significant service providers. Typically, the federal banking agencies communicate to the service providers the findings of the formal examination activities through supervisory letters or reports of examination. In addition, the federal banking agencies make these reports of examination available to financial institution clients of the service providers.

Examiners

The FDIC hires and trains examiners and analysts to conduct IT examinations that include cybersecurity reviews of FDIC-supervised financial institutions.

As of December 31, 2023, the FDIC employed 2,491 staff in its Division of Risk Management Supervision, the majority of which were examiners. Every commissioned examiner must complete IT training sufficient for the examiner to conduct an IT examination at low complexity banks. For financial institutions with more complex IT operations, the FDIC utilizes examiners with experience and training to review such complex IT environments. Examiners are supported by IT Specialists in each regional office, a team of IT Examination Analysts (some of whom specialize in particular areas of IT risk management), and IT and Cyber Risk Management Analysts with specialized training and experience in IT and cybersecurity matters.

As of December 31, 2023, the FDIC employed 314 IT examiners, risk management examiners designated as IT Subject Matter Experts, IT Examination Analysts, and Cyber Risk Management Analysts. This staffing level represents a 2.9% increase in IT/cyber-related examiners and analysts from year-end 2022. However, the number of IT/cyber-related employees has declined by 13.4 percent over a two-year period, compared to the number of such employees as of December 31, 2022. This decline over the last two years reflects retirement-eligible staff and external challenges for technology expertise. The FDIC is taking action to address negative staffing trends, including a review and adjustment of compensation.

Examiner Education and Instruction

The FDIC, as a member of the FFIEC, participates in the publishing of the FFIEC Information Technology Examination Handbook (Handbook).[60] The Handbook consists of several booklets focused on operational risk issues, including information security, to assist examiners in evaluating financial institution and service provider risk management processes. The Handbook also provides examination procedures to assist examiners in evaluating more complex IT risk management environments. The FFIEC periodically publishes updates to the Handbook. For example, in 2021 the FFIEC published the *Architecture, Infrastructure, and Operations (AIO)* booklet, which sets forth principles and practices for financial institution's management of information technology architecture, infrastructure, and operations.

The FDIC participates in the development of FFIEC professional development programs to provide updates on cyber threats and controls to supervisory staff as well as a formal development program that combines traditional training with coached on-the-job experiences for those FDIC examiners who desire to specialize in IT examinations.[61] Recent FFIEC professional development programs addressing cybersecurity and resilience issues included annual Information Technology (August 2023) and Payment Systems Risk (October 2023) conferences.[62]

In addition, FDIC advanced IT development programs provide the opportunity for participants to obtain an IT subject matter expert credential at the intermediate or advanced levels. Examiners with these credentials examine more complex financial institutions and service providers, and build the knowledge, skills, and abilities to compete for higher-graded examiner positions.

As needed, FDIC subject matter experts provide technical training sessions that focus on an exigent threat or vulnerability, such as MOVEit file transfer application and Citrix Bleed vulnerabilities. In addition, FDIC supervisory staff periodically communicates to FDIC examiners and other employees regarding novel cyber threats and vulnerabilities, which may potentially impact FDIC-supervised financial institutions. For example, during 2023 the FDIC distributed advisories to its examiners on the topics of the CITRIX bleed, 3CXDesktopApp, and MOVEit file transfer application vulnerabilities.

Examination Work Programs

Examiners use a standardized work program to guide them through examinations of a financial institution's IT risk management, including the examination of cybersecurity and other operational risk-related matters. The *Information Technology Risk Examination Program (InTREx)* is an interagency examination program governed by the FDIC, FRB, and state financial services regulators. The FDIC, along with the other regulators, updates InTREx periodically to reflect developments in technology, emerging risks, changes in regulatory guidance, and industry trends. For example, effective September 29, 2023, the FDIC, along with FRB and state-bank regulators, updated the *InTREx* program to (i) improve the Audit module's usability; (ii) specify

[60] FFIEC, *FFIEC IT Handbook InfoBase*, https://ithandbook.ffiec.gov/.
[61] FDIC, *Continuing IT Training Program*, https://www.fdic.gov/regulations/examiner/it/training_path.html.
[62] FFIEC, Examiner Education Office, https://www.ffiec.gov/exam/courses.html.

compliance review steps relative to the Computer Security Incident Notification Rule (consistent with Part 304 Subpart C); (iii) provide more specificity regarding service provider reports of examination; and (iv) update links to topical references.

Occasionally, the FDIC develops risk-targeted work programs to assess multiple financial institutions or significant service providers (referred to as a "horizontal review") during a specified period. Based on results from horizontal reviews, the FDIC piloted in 2023 technical examination aids designed to focus examiners on certain controls found to be effective against ransomware attacks.

Large and Complex Institution Cyber, Information Technology and Operational Resiliency

The Division of Complex Institution Supervision and Resolution (CISR), through its Cyber, Information Technology, and Operational Resilience Section, participates in on-site targeted reviews, horizontal examinations, and other supervisory activities to assess the adequacy of cybersecurity, and information technology at those FDIC-insured financial institutions with assets greater than $100 billion that are not supervised directly by the FDIC.

For example, the FDIC, FRB, and OCC jointly conduct horizontal cybersecurity reviews of the eight U.S. global systemically important banks as part of an Interagency Coordinated Cybersecurity Review program to support effective cybersecurity supervision across these systemically important financial institutions. Through the coordination, alignment, and strategic deployment of interagency subject matter experts, the agencies seek to increase efficiencies and achieve greater focus on the most significant cybersecurity risks at these systemically important banks.

Strengthening Cybersecurity in Coordination with Other Agencies

The FDIC collaborates with other government entities (e.g., other federal banking agencies, state banking authorities, U.S. Department of the Treasury, DHS, Federal law enforcement agencies, and regulators in other jurisdictions) and private sector organizations to understand cybersecurity risks and keep its supervision activities current.

Timely and responsive coordination among financial services regulators is an integral part of the FDIC's supervisory program and critical to support the resilience of the U.S. financial system. The FDIC is active in FFIEC efforts to publish resources for examining cybersecurity at financial institutions and to provide information to bankers that can be helpful in cybersecurity risk management. Such coordination includes targeted initiatives for responding to emerging threats and specific operational risks. For example, the federal banking agencies prioritized collaboration in response to the Apache Log4J vulnerability (2021) and the MOVEit file transfer application vulnerability (2023) that posed significant threats to firms across the economy broadly, including financial services. These collaborations resulted in unified communications by the federal banking agencies of information regarding these vulnerabilities to the industry and examination teams to support awareness of the risk, effective mitigation techniques, and potential signs of compromises.

The FDIC addresses broader financial sector cybersecurity risks through participation in organizations such as the FBIIC, and coordination with groups such as the Financial Services Sector Coordinating Council (FSSCC).[63] The FSSCC is comprised of approximately 70 private sector firms representing financial trade associations, utilities, and major financial services firms. In 2015, the FBIIC and FSSCC jointly created the Financial Services Sector Specific Plan (Plan), which articulates a public/private partnership to collaborate on initiatives to strengthen the resilience of the financial services sector. The Plan brings together a network of financial services sector companies; sector trade associations; federal government agencies; financial regulators; state, local, tribal, and territorial governments; and other government and private sector partners. This engagement has resulted in creating coordinated incident response plans, the Hamilton series of tabletop exercises to practice public and private sector response to cyber incidents, and other initiatives with the financial sector.

The FDIC collaborates with law enforcement and other agencies through several venues. These engagements provide the FDIC with a better understanding of cybersecurity threats so examinations and other supervisory activities remain current.

The FDIC has engaged the private sector on cybersecurity-related issues through various organizations and forums including the FS-ISAC[64] and the Analysis and Resilience Center.[65]

On the international front, the FDIC engages with other jurisdictions and international regulatory organizations on cybersecurity issues. The FDIC participates in a Basel Committee on Banking Supervision (BCBS) work stream on operational risks, including cybersecurity risks that may arise from financial institutions' reliance on third party service providers such as cloud service providers. An example of the FDIC's international engagement is collaborating on the 2023 and 2024 BCBS efforts to develop updated supervisory principles for financial institutions in the area of third-party risk management, including management of information and cyber security risks arising from third-party relationships. Another example of international engagement is the FDIC collaboration with the BCBS on the 2021 BCBS *Newsletter on Cyber Security*, which highlights the importance of banks adopting frameworks for cyber-risk management aligned with widely accepted industry standards.

NIST Cybersecurity Framework

The NIST Cybersecurity Framework (CSF) is widely used by organizations of all types to support their management of cyber risk and to assess cybersecurity preparedness of critical operations, core business lines, and other operations. The FDIC and other FFIEC members encourage financial institutions to use such a standardized approach for conducting cybersecurity preparedness self-assessments.[66] On February 26, 2024, NIST released version 2.0 of the CSF. This version expanded the CSF's core guidance to include a new govern function, and it updates all of the CSF functions with new and

[63] Financial Services Sector Coordinating Council, https://fsscc.org/.
[64] Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.
[65] Analysis and Resilience Center, https://systemicrisk.org/.
[66] FFIEC, *FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness*, https://www.ffiec.gov/press/pr082819.html.

revised examples of practices to assist a company in achieving its cyber security outcome. [67] The FDIC is considering the potential impact of this new version of NIST CSF, and the FDIC will adjust its examination work programs and other cyber-related issuances as appropriate.

Industry Efforts

The FDIC has observed that the financial services industry has continued its efforts to prepare for, prevent, and respond to cybersecurity threats. On the individual institution level, supervised financial institutions have taken steps to address regulatory examination findings and recommendations. At the sector level, recent examples of industry-led efforts include: (1) updates to the Cyber Risk Institute's (CRI) Profile,[68] (2) continued adoption of the Sheltered Harbor standards and certification process,[69] and (3) updates to the Global Resilience Federation's Operational Resilience Framework.[70]

Efforts to Respond to OIG Cybersecurity-Related Findings and Recommendations

The FDIC OIG is an independent office that conducts audits, evaluations, investigations, and other reviews of FDIC programs and operations 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. There have been several OIG reports issued that relate to the FDIC's supervision of cybersecurity at financial institutions and service providers.

In 2023, the FDIC OIG released a report on its assessments of the FDIC's efforts to alert supervised financial institutions of relevant cyber and other threat and vulnerability information.[71] This OIG report included a number of recommendations including that the FDIC (i) share FDIC-developed threat and vulnerability information with financial institutions or other financial sector entities, and (ii) improve controls over the recording of computer-security incidents reported by banks and service providers. The FDIC concurred with these OIG recommendations and is taking action to address all of the report's recommendations by June 30, 2024.

In 2022, the OIG released two reports that address the FDIC's supervision of cybersecurity at financial institutions and service providers: the *Sharing of Threat Information to Guide the Supervision of Financial Institutions (AUD-22-003)*[72] and *Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program (AUD-23-001)*.[73] As detailed in the above Policies and Procedures section of this report,

[67] *NIST Cybersecurity Framework version 2.0*, https://www.nist.gov/cyberframework.
[68] CRI, Press Release, *CRI Issues Profile Version 2.0,* February 29, 2024, https://cyberriskinstitute.org/cri-issues-profile-version-2-0/
[69] Sheltered Harbor, https://www.shelteredharbor.org/.
[70] Global Resilience Framework, Press Release, *The Operational Resilience Framework Introduces New Maturity Model,* November 2, 2023, https://www.grf.org/news/the-operational-resilience-framework-introduces-new-maturity-model
[71] FDIC OIG Report, "*Sharing of Threat and Vulnerability Information with Financial Institutions*," August 2023, https://www.fdicoig.gov/sites/default/files/reports/2023-08/EVAL-23-002%20REDACTED%20FINAL_0.pdf.
[72] FDIC OIG, *Sharing of Threat Information to Guide the Supervision of Financial Institutions*, January 2022, https://www.fdicoig.gov/sites/default/files/reports/2022-08/AUD-22-003_Redacted.pdf.
[73] FDIC OIG, *Implementation of the FDIC's Information Technology Risk Examination Program,* January 2023, https://www.fdicoig.gov/sites/default/files/reports/2023-02/AUD-23-001.pdf.

the FDIC undertook several initiatives during this reporting period that build upon and strengthen internal information sharing, the InTREx examination work program, and IT supervision generally, including issuing an update to the InTREx procedures in September 2023.

In addition, the OIG identified "Mitigating Cybersecurity Risks at Banks and Third Parties," and "Fortifying IT Security at the FDIC" as two top management challenges for the FDIC in an appendix to the FDIC's 2022 Annual Report.[74] As discussed throughout this report, the FDIC continues to use its authorities to mitigate cybersecurity risks in the banking sector and strengthen internal operations to protect the agency's data and other resources.

Threats

Tactical

Tactical cybersecurity threats are those that pose risk in the near-term. According to the 13th Annual Ernst & Young (EY) Global Bank Risk Management Survey, cybersecurity risk was the top near-term risk for banks.[75] Furthermore, the International Monetary Fund's 2024 Global Financial Stability Report[76] cited that extreme losses from cyber incidents are increasing and such losses could potentially cause funding problems for targeted companies and even jeopardize their solvency.

Geopolitical events continue to increase the likelihood of cyberattacks on banks. Events like the Israel-Hamas conflict and the war in Ukraine have led to increased cyberattacks targeting critical infrastructure around the world. These attacks include politically motivated distributed denial-of-service attacks,[77] targeting of information technology components and software, and targeting of U.S. critical infrastructure networks by nation-states, nation-state proxies, or hacktivists.

Ransomware continues to pose a significant threat to U.S. critical infrastructure sectors, including finance and banking. These data encryption and exfiltration attacks can result in a target financial company's inability to access its critical business and customer data. Malicious actors typically leverage known software vulnerabilities, compromised credentials, and phishing emails to gain access to networks and deploy ransomware. Ransomware developers and operators continue to advance their tactics and tools, even offering services to others through a Ransomware-as-a-Service (RaaS) model, making it easier for less technically experienced cybercriminals to launch attacks. In 2023, ransomware actors largely shifted from data encryption to data exfiltration techniques, demanding that victim financial companies pay a ransom to keep them from exposing stolen data. In either scenario, ransomware can disrupt core business activities, result in operational outages, threaten the confidentiality of customer data, and lead to a loss of customer and counter-party confidence in the financial company.

Cyber threats to third-party providers of software and computing services remain an important source of risk to the financial sector. Security risks arising from compromised third-party

[74] FDIC, *2022 Annual Report – Appendix 7*, https://www.fdic.gov/about/financial-reports/reports/2022annualreport/ar22section7.pdf.
[75] Ernst & Young/Institute of International Finance, "13th Annual EY/IIF Global Bank Risk Management Survey," February 6, 2024.
[76] International Monetary Fund, "Global Financial Stability Report," April 9, 2024.
[77] Microsoft, "Digital Defense Report," October 2023.

software include disclosure of credentials or confidential data, corruption of data, installation of malware, and application outages. These problems can result in lost time, money, and customer trust. IBM's Cost of a Data Breach Report 2023[78] reflected that 15 percent of organizations identified a supply chain compromise, and 12 percent identified a software supply chain attack, as the source of a data breach.

An example of a supply chain threat that plagued the financial sector was the compromise by Russian-based Cl0p ransomware group of a since-patched vulnerability in a widely used file transfer application software called MOVEIt. The MOVEIt campaign targeted the U.S. financial sector and other enterprises globally with estimates of 2,618 organizations and 77 million individuals affected.

Strategic

Strategic cybersecurity threats are those that are more likely to result in disruptions in the long-term but require current preparation and planning to prevent disruption and add resilience. For example, malicious actors are leveraging generative artificial intelligence (AI) technologies to circumvent identity- and authentication-based financial institution network defenses and to perpetrate other frauds. These perpetrators of financial crimes are increasingly using AI to create fraudulent or altered documentation, audio files, and video recordings, leading to increasing number of fraud cases.[79] The pervasiveness of generative AI tools allow malicious actors to easily leverage the technology to create more convincing or realistic content or materials to further fraud schemes.[80] Generative AI, including large language models, can augment live videos via "deepfakes" or voice cloning tools, making it more difficult for financial institutions to discern real versus fraudulent (including synthetic) identities during customer account opening, processing of transactions, or verification processes.

Another example of a strategic cybersecurity threat is the continuing development of quantum computing technology. Quantum computers use a different computing architecture that can solve certain types of problems much faster, including some encryption algorithms. Once fully developed, it is anticipated that quantum computing will provide substantially greater computing speed and power, as compared to current models. Quantum computing is expected to eventually weaken or incapacitate the current encryption methods that the financial sector uses to secure the integrity and confidentiality of its networks and data against cyber attackers.

Conclusion

The FDIC appreciates the opportunity to provide this report on the FDIC's efforts to address cybersecurity threats and its efforts in partnership with other private and public sector stakeholders.

[78] IBM, "Cost of a Data Breach Report 2023," December 2023.
[79] Sift, "Q2 2023 Digital Trust & Safety Index – Fighting Fraud in the Age of AI and Automation," June 22, 2023.
[80] Precedence Research, "Generative AI Market Growth Is Booming With 27.02%," July 11, 2023.