2025 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.[1]

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 institutions");[2] 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[3] (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 institutions and by examining services provided by certain service providers. More specifically, the FDIC evaluates 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 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 exploit vulnerabilities in cybersecurity to harm others requires constant vigilance and agility. The FDIC will continue to collaborate with stakeholders to maintain and strengthen its cybersecurity programs.

[1] Section 108 of the Consolidated Appropriations Act 2021 requires each banking regulator to annually submit a report to the Committee on Financial Services of the House of Representatives and the Committee on Banking, Housing, and Urban Affairs of the Senate that provides a detailed explanation of measures undertaken to strengthen cybersecurity within the financial services sector and with respect to the functions of the regulator, including the supervision and regulation of financial institutions and, where applicable, third-party service providers. Consolidated Appropriations Act, 2021, Pub. L. No. 116-260, Div. Q, Title 1, § 108, 134 Stat. 2173 (2020).

[2] 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. § 1831p-1), and state savings associations.

[3] Federal Information Security Modernization Act of 2014, Pub. L. No. 113-283, 128 Stat 3073 (2014).

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,[4] 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 1360.01, *Information Security Program*, was updated in 2024 to set forth specific roles and responsibilities for ensuring adequate levels of protection for FDIC information systems and that the information processed, stored, or transmitted are in compliance with FISMA, OMB Circular A-130[5], and NIST Special Publication (SP) 800-37.[6]

In 2024, FDIC also 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 in the FDIC's Information Systems Security Management Program. The updated policies include FDIC Directive 1360.09, *Protecting Information* (March 2024), which sets forth a policy on the rules of behavior for protecting information according to its level of sensitivity. In addition, Directive 1320.04, *Software Configuration Management* (March 2024), sets forth a policy and responsibilities for ensuring effective, efficient, and consistent software configuration management (SCM) of FDIC applications and system software products throughout their lifecycles. Other key areas of focus in 2024 included continuing efforts to implement a Zero Trust Architecture,[7] strengthening the security of the FDIC's cloud platforms, continuing to improve incident response capabilities, and maturing the implementation of the CISA Continuous Diagnostics and Mitigation (CDM) Program.

---

[4] Exec. Order No. 14028, 86 FR 26633 (2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

[5] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, *Managing Information as a Strategic Resource* (2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.

[6] National Institute of Standards and Technology (2018) *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*. (Department of Commerce, Washington, D.C.) NIST Special Publication 800-37, Revision 2 December 2018, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-37r2.pdf.

[7] OMB Memorandum, M-22-09 describes Zero Trust as follows: "The foundational tenet of the Zero Trust Model is that no actor, system, network, or service operating outside or within the security perimeter is trusted. Instead, we must verify anything and everything attempting to establish access." Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.

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 FDIC's Information Security Program – 2024,*[8] auditors concluded that "the FDIC established several 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 2024 was Level 4 (*Managed and Measurable*),[9] 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 to the OIG report, FDIC management concurred with three recommendations related to updating the Plans of Action and Milestones (POA&M) Management and Acceptance of Risk Process document, reviewing and analyzing system audit records, and remediating technical issues within the FDIC's Learning Management System. In addition, the FDIC closed two out of the four recommendations from prior-year FISMA audits and is working to complete the necessary corrective actions to close the two remaining unimplemented recommendations from 2022 and 2023 FISMA Audit reports.

Implementation

The FDIC has an established information security program that continues to evolve to meet new challenges. In 2024, the FDIC completed certain actions to strengthen its security controls, such as finalizing the processes and procedures related to supply chain risk management (SCRM) and completing actions to address the technical issues preventing enforcement of security and privacy training compliance.

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

- Continued efforts to implement a Zero Trust Architecture in accordance with Executive Order 14028 and aligned to the CISA's Zero Trust Maturity Model;
- Strengthened the security of cloud platforms through the development of platform specific hardening guides and security implementation plans;
- Continued the implementation of CISA's CDM program;
- Enhanced the FDIC's information security and privacy continuous monitoring program by leveraging automation and integration with information sources;
- Developed an enterprise-wide penetration testing service focused on identifying potential vulnerabilities in the FDIC's mission-essential and mission-critical systems;
- Continued to improve incident response capabilities by establishing new processes for managing incidents related to the loss of data;
- Implemented improvements to IT security governance by updating multiple agency level policies and directives; and

[8] FDIC Office of Inspector General Report, No. EVAL-24-07, *The FDIC's Information Security Program – 2024* (September 2024), https://www.fdicoig.gov/sites/default/files/reports/2025-03/FISMA%202024-EVAL-24-07%20-%20Final%20Report%20-%20Redacted.pdf.
[9] Council of the Inspectors General on Integrity and Efficiency, *FY 2024 IG FISMA Metrics Evaluator's Guide*, (2024), https://www.cisa.gov/sites/default/files/2024-05/FY%202024%20IG%20FISMA%20Metrics%20Evaluation%20Guide%20Final.pdf.

- Developed an adoption strategy for FDIC's centralized identity, credential, and access management (ICAM) solution and expanded the capabilities of this solution to improve access for public users.

Despite this progress, there are areas where the FDIC needs to improve. For example, the FDIC needs to continue to improve its SCRM strategy, audit logging, POA&M management, privileged account management, and role-based training requirements. 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 539 security events reported to the SRT from October 1, 2023 through September 30, 2024. 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 under OMB guidance.[10] During the same period, the FDIC reported 137 of these incidents, which included 41 breaches, to the Security Operations Center (SOC) of CISA following the CISA Federal Incident Notification Guidelines.[11] Most of these were "Improper Usage" incidents and involved employee activities such as individuals emailing potentially sensitive information to their own personal e-mail accounts or inadvertently sending emails to incorrect recipients. All the incidents reported to CISA received a Cyber Incident Scoring System (NCISS) priority score of either Baseline – Negligible or Baseline – Minor.[12]

EO 14028, *Improving the Nation's Cybersecurity*,[13] outlines several cybersecurity measures and requirements intended to strengthen 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 helps to ensure 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 migration of the Federal government's IT infrastructure 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.*

[10] OMB Guidance describes a major incident as "any incident that is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States or to the public confidence, civil liberties, or public health and safety of the American people;" or "[A] breach that involves personally identifiable information (PII) that, if exfiltrated, modified, deleted, or otherwise compromised, is likely to result in demonstrable harm to the national security interests, foreign relations, or the economy of the United States, or to the public confidence, civil liberties, or public health and safety of the American people." Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements* (2019), https://www.whitehouse.gov/wp-content/uploads/2019/11/M-20-04.pdf.

[11] Cybersecurity and Infrastructure Security Agency, *Federal Incident Notification Guidelines* (2017), https://www.cisa.gov/federal-incident-notification-guidelines.

[12] CISA's *Federal Incident Notification Guidelines* describe a Baseline - Minor incident as one that is "[H]ighly unlikely to affect public health or safety, national security, economic security, foreign relations, civil liberties, or public confidence. And a Baseline – Negligible as an "Unsubstantiated or Inconsequential event." Cybersecurity and Infrastructure Security Agency, *Federal Incident Notification Guidelines* (2017), https://www.cisa.gov/federal-incident-notification-guidelines.

[13] Exec. Order No. 14028, 86 FR 26633 (2021), https://www.federalregister.gov/documents/2021/05/17/2021-10460/improving-the-nations-cybersecurity.

Government Toward Zero Trust Cybersecurity Principles,[14] 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 Federal government's defenses against increasingly sophisticated and persistent threat campaigns. The FDIC has responded to all required actions under the memorandum.

- *Improve software supply chain security*. The EO seeks to improve Federal government software security by requiring the Secretary of Commerce and others to establish baseline security standards for development of software sold to the Federal government. 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,*[15] and followed with M-23-16, *Update to Memorandum M-22-18 Enhancing Software Supply Chain through Secure Software Development Practices,*[16] 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 required actions under these memoranda.
- *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*,[17] 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 required actions under these memoranda.
- *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*

[14] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles* (2022), https://www.whitehouse.gov/wp-content/uploads/2022/01/M-22-09.pdf.
[15] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (2022), https://www.whitehouse.gov/wp-content/uploads/2022/09/M-22-18.pdf.
[16] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-23-16, *Update to Memorandum M-22-18, Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (2023), https://www.whitehouse.gov/wp-content/uploads/2023/06/M-23-16-Update-to-M-22-18-Enhancing-Software-Security.pdf.
[17] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-22-01, Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems through Endpoint Detection and Response (2021), https://www.whitehouse.gov/wp-content/uploads/2021/10/M-22-01.pdf.

Cybersecurity Incidents,[18] 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 and Executive Branch departments and agencies. CISA published *Guidance for Implementing M-21-31: Improving the Federal Government's Investigative and Remediation Capabilities*[19] 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-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*,[20] 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 continues to use data collected from agency FISMA submissions to improve the security outcomes of Federal IT systems, in accordance with the National Cyber Strategy's call to modernize systems and continue to build out collective defense in four key areas:

- *Measuring Zero Trust implementation*. Agencies are required to take discrete, time-bound steps by fiscal year 2024 to meet the goals of EO 14028 and M-22-09.
- *Clear, actionable, and outcome-focused data*. M-22-05[21] initiated significant changes in the Federal government's approach to FISMA oversight and Chief Information Officer (CIO) and Inspector General (IG) metrics collection, and OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*, continued to refine that approach. This memorandum builds on the foundation established in M-22-05 to 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 fiscal year 2024 CIO metrics will fully automate certain reporting.
- *Ensuring input from across the Federal enterprise*. OMB and CISA will continue to support the efforts of the CISO Council's FISMA Metrics Subcommittee, which is tasked with advising OMB on possible refinements and improvements to FISMA guidance and metrics.

---

[18] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (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.

[19] Cybersecurity and Infrastructure Security Agency, *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.

[20] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements* (2023), https://bidenwhitehouse.archives.gov/omb/information-for-agencies/memoranda/.

[21] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements* (2021), https://www.whitehouse.gov/wp-content/uploads/2021/12/M-22-05-FY22-FISMA-Guidance.pdf.

- *Improving security-privacy coordination*. While independent and separate disciplines, security and privacy also have a close relationship as described in OMB Circular A-130, *Managing Information as a Strategic Resource*.[22] Coordination across these disciplines is essential to managing security and privacy risks and to complying with applicable requirements as outlined in this memorandum.

The FDIC reported the fiscal year 2024 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.

Additionally, OMB issued the following Memoranda:

- *OMB Memorandum M-24-10, Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence.*[23] M-24-10 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 the actions required under this memorandum.
- *OMB Memorandum M-24-14, Administration Cybersecurity Priorities for the Fiscal Year 2026 Budget*.[24] M-24-14 outlines the prior administration's cross-agency cybersecurity investment priorities for formulating fiscal year 2026 budget submissions to OMB focused on the National Cybersecurity Strategy (NCS) five pillars to enhance the Nation's cybersecurity posture. The FDIC has responded to all applicable actions required under this memorandum.
- *OMB Memorandum M-24-15, Modernizing the Federal Risk and Authorization Management Program (FedRAMP)*.[25] M-24-15 provides guidance on (1) the scope of FedRAMP, (2) requirements for the use of the program by Federal agencies, (3) responsibilities of the FedRAMP Board and the program management office (PMO) at GSA, and (4) promoting consistency in the assessment, authorization, and use of secure cloud services by Federal agencies. The FDIC has incorporated the requirements of this memo into its system authorization process. The FDIC is also working to offboard legacy cloud service providers who do not have FedRAMP authorization.
- *OMB Memorandum M-24-18, Advancing the Responsible Acquisition of Artificial Intelligence in Government*.[26] M-24-18 directs agencies to improve their capacity for the responsible acquisition of AI. It contains new requirements and guidance for agencies on establishing meaningful cross-functional and interagency collaboration to reflect new AI responsibilities, managing AI risk and performance, and promoting a

[22] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Circular A-130, *Managing Information as a Strategic Resource* (2016), https://obamawhitehouse.archives.gov/sites/default/files/omb/assets/OMB/circulars/a130/a130revised.pdf.
[23] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-24-10, *Advancing Governance, Innovation, and Risk Management for Agency Use of Artificial Intelligence* (2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/03/M-24-10-Advancing-Governance-Innovation-and-Risk-Management-for-Agency-Use-of-Artificial-Intelligence.pdf.
[24] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-24-14, *Administration Cybersecurity Priorities for the FY 2026 Budget* (2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/FY26-Cybersecurity-Priorities-Memo_Signed.pdf.
[25] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-24-15, *Modernizing the Federal Risk and Authorization Management Program (FedRAMP)* (2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/07/M-24-15-Modernizing-the-Federal-Risk-and-Authorization-Management-Program.pdf.
[26] Office Of Mgmt. & Budget, Exec. Office of the President, OMB Memorandum M-24-18, *Advancing the Responsible Acquisition of Artificial Intelligence in Government* (2024), https://bidenwhitehouse.archives.gov/wp-content/uploads/2024/10/M-24-18-AI-Acquisition-Memorandum.pdf.

competitive AI market with innovative acquisition. The FDIC is working to respond to all the applicable actions required under this memorandum.

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.

The FDIC fully complied with the two BODs and two EDs issued by CISA in fiscal year 2024:

- *ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*.[27] 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 results in full compromise of target information systems by allowing a malicious actor to move laterally across, perform data exfiltration, and establish persistent system access. CISA has determined these vulnerabilities pose an unacceptable risk to Federal civilian executive branch (FCEB) agencies and require emergency action. The FDIC completed all actions required under the ED.
- *Supplemental Direction V1: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*.[28] The Supplemental Direction V1 supersedes action 4 in ED 24-01, which is applicable to any Federal agency running Ivanti Connect Secure or Ivanti Policy Secure solutions. Threat actors continue to leverage the vulnerabilities in these products to capture credentials and drop webshells that enable further compromise of enterprise networks. Some threat actors have recently developed workarounds to earlier mitigation and detection methods and have been able to exploit weaknesses, move laterally across, 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 actions required under Supplemental Direction V1.
- *Supplemental Direction V2: ED 24-01: Mitigate Ivanti Connect Secure and Ivanti Policy Secure Vulnerabilities*.[29] Supplemental Direction V2 supersedes Supplemental Direction V1 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 and that enables an attacker to access restricted resources without authentication. Ivanti released new

[27] Cybersecurity and Infrastructure Security Agency, Emergency Directive 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.
[28] Cybersecurity and Infrastructure Security Agency, 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.
[29] Cybersecurity and Infrastructure Security Agency, 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.

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 ICT. The FDIC completed all actions required under Supplemental Direction V2.

- *ED 24-02: Mitigating the Significant Risk from Nation-State Compromise of Microsoft Corporate Email System*.[30] 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, beginning in January 2024: *Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*[31] and *Update on Microsoft Actions Following Attack by Nation State Actor Midnight Blizzard*.[32] 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. Therefore, CISA has required 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 actions required under this ED and continues to coordinate with CISA as new information concerning this event is discovered.
- *BOD 25-01: Implementing Secure Practices for Cloud Services*.[33] Malicious threat actors have increasingly targeted cloud environment and evolved their tactics to gain initial cloud access. In recent cybersecurity incidents, improper configuration of security controls in cloud environments introduced substantial risk and resulted in security compromises. To combat these threats, CISA initiated the Secure Cloud Business Applications (SCuBA) project. Through the SCuBA project, CISA developed secure configuration baselines, which provide consistent and manageable cloud security configurations and assessment tools that allow agencies and CISA to improve security for FCEB agency assets hosted in cloud environments. BOD 25-01 requires agencies to implement a set of SCuBA security configuration baselines for certain software as a service (SaaS) products widely used by FCEB agencies; deploy CISA developed automated configuration assessment tools to measure against the required baselines; integrate CISA's continuous monitoring infrastructure; and remediate deviations from the secure configuration baselines. These baselines help to reduce the risks highlighted by recent cyber events and increase the resiliency of FCEB agencies against cyber threats. The FDIC is working to respond to actions required under BOD 25-01. As part of the BOD 25-01, CISA also released *Implementation Guidance for Implementing Secure Practices for Cloud Services.* This implementation guidance provides FCEB agencies with

[30] Cybersecurity and Infrastructure Security Agency, 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.
[31] Microsoft Security Response Center, *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/.
[32] Microsoft Security Response Center, *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/.
[33] Cybersecurity and Infrastructure Security Agency, Binding Operational Directive BOD 25-01, *Implementing Secure Practices for Cloud Services* (2024), https://www.cisa.gov/news-events/directives/bod-25-01-implementing-secure-practices-cloud-services.

additional context and instructions for implementing the requirements from BOD 25-01. The FDIC is working to respond to all the 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 (CSF) 2.0[34] 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 sector cybersecurity and resilience. This section also discusses how the FDIC reviews FDIC-supervised 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 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 Financial Institutions Examination Council (FFIEC)[35] websites[36] for reference by financial institutions and other entities, and periodically update these resources.

[34] National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. (Department of Commerce, Washington, D.C.) *NIST CSWP 29* (February 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.

[35] 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.

[36] 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.

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 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 the 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.[37] These Guidelines set forth standards for institutions regarding administrative, technical, and physical safeguards to protect the security, confidentiality, and integrity of customer information.

Computer-Security Incident Notification Rule[38]

Effective May 1, 2022, banking organizations, including FDIC-supervised 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. Computer-security incidents reported under this rule can result from cyberattacks, such as destructive malware, or from non-cyberattack incidents, such as the failure of hardware and software at a bank. For the annual period ending September 30, 2024, the majority of all incident notices received from FDIC-supervised institutions related to crimeware and supply chain compromise incidents. This analysis is based on notices submitted pursuant to the Computer-Security Incident Notification Rule as well as other incident notices voluntarily submitted by institutions.

As a principal member of the Cyber Incident Reporting Council (CIRC),[39] formed in response to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[40] the FDIC is working with CISA and other regulatory agencies on a multi-year

[37] 15 U.S.C.A. §§ 6801, 6805(b) (West, Westlaw through Pub. L. No. 119-12).
[38] 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.
[39] 6 U.S.C. § 681f (West, Westlaw through Pub. L. No. 119-12).
[40] Cyber Incident Reporting for Critical Infrastructure Act of 2022, Pub. L. No. 117-103, Div. Y. 136 Stat 49 (2022).

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 the DHS report to Congress entitled "Harmonization of Cyber Incident Reporting to the Federal Government."[41] During 2023 and 2024, the FDIC consulted on a CISA notice of proposed rulemaking, published in April 2024, which requests public comment on key cyber incident definitions and reporting thresholds.[42]

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 guidance issued over the past four years that include discussions of cyber-risk are:

- 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.[43] 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 August 2021, the FFIEC member entities published guidance on authentication and access to financial institution services and systems,[44] which sets forth examples of risk management principles and practices for effective authentication of customers, employees, and other users. Effective authentication of customers, employees, and other users into IT 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

[41] DHS, *Harmonization of Cyber Incident Reporting to the Federal Government (*September 19, 2023), https://www.dhs.gov/publication/harmonization-cyber-incident-reporting-federal-government.
[42] *Cyber Incident Reporting for Critical Infrastructure Act (CIRCIA) Reporting Requirements,* 89 Fed. Reg. 23644-01 (proposed April 4, 2024) (to be codified at 6 C.F.R. pt. 226).
[43] Joint Press Release, FDIC, Federal Reserve Board, OCC, *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.
[44] 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.[45] FFIEC, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement* (November 3, 2014), https://www.ffiec.gov/sites/default/files/media/press-releases/2014/FFIEC_Cybersecurity_Statement.pdf.

threats and vulnerabilities.[45] This recommendation has been highlighted in subsequent releases. The FS-ISAC is a non-profit, information-sharing forum established by financial services industry participants to facilitate public-private 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 institutions inform their defensive activities and remediate system weaknesses. FDIC supervisory staff also consider other information sources including Suspicious Activity Reports,[46] 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 institutions, examined service providers, and FDIC employees.

Over the past four years, the FDIC, along with other federal and state regulators, provided information to financial institutions regarding the following significant alerts and advisories:

- CISA and National Security Agency (NSA) advisory titled, *People's Republic of China State-Sponsored Actors Compromise and Maintain Persistent Access to U.S. Critical Infrastructure* (February 29, 2024).
- CISA, NSA, and other governmental agencies' advisory titled, *Joint Guidance on Identifying and Mitigating Living Off the Land Techniques* (February 29, 2024).
- Announcement from the Department of Commerce's Bureau of Industry and Security regarding its final determination prohibiting Kaspersky Lab, Inc. from directly or indirectly providing anti-virus software and cybersecurity products and services in the United States or to U.S. persons (June 20, 2024).
- FFIEC members' cybersecurity alerts regarding the MOVEit file transfer application vulnerability, including a discussion of potential risks of cyberattacks affecting institutions' third-party relationships and recommendations to remediate these risks (June 6, 2023 and September 18, 2023).

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,[47] a directors' resource portal, director/banker colleges, teleconferences and webinars, community bank resource kits, regional compliance newsletters, and individual assistance to institutions. FDIC

[45] FFIEC, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement* (November 3, 2014), https://www.ffiec.gov/sites/default/files/media/press-releases/2014/FFIEC_Cybersecurity_Statement.pdf.
[46] See, 12 C.F.R. §§ 208.62, 211.5(k), 211.24(f), and 225.4(f) (Federal Reserve) (2024); 12 C.F.R. § 353 (FDIC) (2024); 12 C.F.R. § 748.1(c) (NCUA) (2024); 12 C.F.R. §§ 21.11 and 12 C.F.R. § 163.180 (OCC) (2024); and 31 C.F.R. Chapter X (FinCEN) (2024).
[47] FDIC, *Directors' Resource Center Technical Assistance Video Program*, https://www.fdic.gov/banker-resource-center/technical-assistance-video-program.

technical assistance on the topics of cybersecurity and resilience over the past four years has included:

- *Cybersecurity Awareness instructional videos*. The FDIC produced a technical assistance video that provides background information on cybersecurity and emphasizes the board of directors' role in overseeing cybersecurity efforts. Additionally, on November 30, 2023, 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.
- *Ransomware Program for Small- to Mid-Sized Financial Institutions*. The FDIC collaborated with the Financial and Banking Information Infrastructure Committee[48] (FBIIC) to host a virtual forum on March 1, 2022 regarding ransomware risk and mitigation strategies for small- to mid-sized financial institutions.
- *Computer-Security Incident Notification "Ask the Regulators" Forum*. The FDIC, FRB, and OCC held a webinar on April 28, 2022 for all FDIC-insured institutions and service providers to address industry questions about computer-security incident reporting.
- *Preparing for Post-Quantum Cryptography*. The FDIC collaborated with CISA through the FFIEC to provide all FDIC-insured institutions with the opportunity to participate in a non-public virtual forum on September 23, 2022, 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.

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

- *FIL-7-2025*. The FDIC released FIL-7-2025 to clarify that FDIC-supervised institutions may engage in permissible crypto-related activities without receiving prior FDIC approval. This FIL also states that FDIC-supervised institutions should consider the associated risks, including cybersecurity risks.[49]
- *FFIEC Cybersecurity Resources Guide for Financial Institutions*.[50] The FDIC jointly published an update to the resource guide that provides a variety of free or low-cost cybersecurity-related resources. The updated resource guide now includes ransomware-specific resources.
- *Joint Statement on Heightened Cybersecurity Risk*.[51] Issued in coordination with the OCC to remind institutions of sound cybersecurity management principles.

[48] 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.
[49] FDIC, Financial Institution Letter No. FIL-7-2025, *FDIC Clarifies Process for Banks to Engage in Crypto-Related Activities* (March 28, 2025), https://fdic.gov/news/financial-institution-letters/2025/fdic-clarifies-process-banks-engage-crypto-related.
[50] FFIEC, *Cybersecurity Resources Guide for Financial Institutions* (September 2022 revised November 2022), https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf.
[51] 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.

- *Statement on Risk Management for Cloud Computing Services*.[52] The FFIEC member agencies released this statement to highlight 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.
- *Sound Practices to Strengthen Operational Resilience*.[53] The FDIC, along with the OCC and the FRB, released this joint statement outlining sound practices designed to help large banks increase operational resilience. Examples of risks to operational resilience include cyberattacks, natural disasters, and pandemics.

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 outreach and other publications over the past four years include:

- *U.S. Treasury Unclassified Threat Exchanges.* Beginning in June 2022 and throughout 2024, the FDIC partnered with the U.S. Department of the Treasury (U.S. Treasury) Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) to offer 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 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.
- *Minority Depository Institutions (MDI) and Community Development Financial Institutions (CDFI) Outreach*. The FDIC provided cybersecurity and IT technical assistance to MDIs and CDFIs. Consultation topics throughout 2024 included: Interagency Information Security Standards; cybersecurity preparedness; responding to IT examination matters (e.g., IT governance, IT audit expectations, and business continuity planning); IT patch management; IT asset end-of-life issues; and IT risk assessments. In addition, regional outreach programs included discussions on cybersecurity controls, third-party vendor management, and other IT-related topics.
- *2024 Risk Review*. The FDIC 2024 Risk Review provides financial institutions and the public an overview of banking conditions for 2023 through early 2024 in five broad categories: market risks, credit risks, operational risks, crypto-

[52] Press Release, FFIEC, *FFIEC Issues Statement on Risk Management for Cloud Computing Services* (April 30, 2020), https://www.ffiec.gov/news/press-releases/2020/pr-04-30.
[53] Joint Press Release, Board of Governors of the Federal Reserve System, FDIC, OCC, *Agencies Release Paper on Operational Resilience* (October 30, 2020), www.fdic.gov/news/press-releases/2020/pr20122.html.
[54] Cybersecurity and Infrastructure Security Agency, *Traffic Light Protocol 2.0 User Guide* (2022). https://www.cisa.gov/sites/default/files/2023-02/tlp-2-0-user-guide_508c.pdf.

asset risks, and climate-related financial risks. The 2024 Risk Review's discussion of operational risks discusses risks arising from malicious cybercrime activities, including the challenge of securing new technologies from potential negative impact from cyber threats.[55]

- *Webinar on Sunset of the CAT*. With the other members of the FFIEC, on October 17, 2024, the FDIC participated in an outreach event for the financial services industry on the planned sunset of the Cybersecurity Assessment Tool (CAT). This event included a discussion of the path forward for financial institutions to assess their cybersecurity and other related risks using other government and industry resources. The sunset of the CAT is discussed in more detail below in this report.
- *Webinar on Update to the FFIEC IT Handbook.* With the other members of the FFIEC, on November 7, 2024, the FDIC hosted an industry outreach webinar to provide information regarding the recently published *Development, Acquisition, and Maintenance Booklet* of the *FFIEC Information Technology Examination Handbook*.
- *Threat $potlight Bulletin.* The FDIC issued the first edition of its *Threat $potlight* bulletin. This bulletin was provided to all FDIC-supervised institutions and highlighted recent cybersecurity risks and financial crime schemes. This information was based on open sources of cybersecurity threats, incident notices and cyber events involving FDIC-supervised institutions, and information related to emerging financial crimes. The *Threat $potlight* bulletin is intended to support the development of internal controls, policies, procedures, and risk assessments that can be used to protect institutions, employees, and customers.[56]
- *FDIC Directors' College and Regional Risk Conferences.*[57] Throughout 2024, the FDIC continued to organize 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 authorities and industry trade groups.
- *Ask the Regulators Webinar: Third-Party Risk Management*. On July 26, 2023, the FDIC, along with the OCC and FRB, offered a webinar to industry on the recently updated supervisory guidance for third-party risk management.
- *Ransomware Webinar*. On October 31, 2023, 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, including new data destruction tactics and mitigation recommendations.

[55] Press Release, FDIC, *FDIC Publishes 2024 Risk Review* (May 22, 2024), https://www.fdic.gov/news/press-releases/2024/fdic-publishes-2024-risk-review.
[56] *Threat $potlight*, Fall Edition 2024. (Publication distributed only to supervised financial institutions.)
[57] FDIC, Directors College Program (updated March 31, 2022), https://www.fdic.gov/directors-college-program.

- *Treasury Cloud Report*. In 2023, the FDIC contributed views and perspectives to the U.S. Treasury in connection with its report titled, *Financial Services Sector's Adoption of Cloud Services.*[58] The U.S. 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. Following the issuance of the report, U.S. 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. FDIC staff is contributing to a number of work streams of the CSSG. For example, in 2024, FDIC staff contributed views to the development of the U.S. Treasury's *Shared Cloud Lexicon and Terminology*.[59]

Implementation

The FDIC examines IT risk management practices, including cybersecurity, at each FDIC-supervised institution. The focus of these 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.[60] Examiners also incorporate the IT rating into the management component of the CAMELS rating.[61] During 2024, the FDIC conducted 1,205 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 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[62] to address weak operating practices identified during the examination.

Separately, the FDIC's Division of Depositor and Consumer Protection examines FDIC-supervised 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 institutions. The FDIC examines the performance of such services jointly with the FRB and OCC. States also join these examinations when there is overlapping authority and interest. These bank service provider

[58] U.S. Dept. of the Treasury, *The Financial Services Sector's Adoption of Cloud Services (*February 8, 2023), https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf.
[59] U.S. Dept. of the Treasury, *Shared Cloud Lexicon and Terminology* (July 17, 2024), https://home.treasury.gov/system/files/216/Shared-Cloud-Lexicon.pdf.
[60] FFIEC, *Supervision of Technology Service Providers Booklet (Appendix A)* (October 2012), https://ithandbook.ffiec.gov/it-booklets/supervision-of-technology-service-providers.
[61] FDIC, RMS Manual of Examination Policies – Basic Examination Concepts and Guideline (March 2022), https://www.fdic.gov/regulations/safety/manual/section1-1.pdf.
[62] FDIC, *FDIC Formal and Informal Enforcement Actions Manual* (updated December 12, 2023), https://www.fdic.gov/regulations/examinations/enforcement-actions/index.html.

examinations frequently include a review of service provider controls designed to defend against advanced cyber threats. During 2024, these examinations included evaluations of risks associated with privileged account access and developments in quantum computing.

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

For 2024, the FDIC established a performance goal to implement strategies to promote enhanced cybersecurity and business continuity within the banking industry. The FDIC achieved this goal through a number of activities in 2024, including: (i) continuing to conduct horizontal reviews that focus on the IT risks in large, complex service providers; (ii) continuing to conduct service provider examinations using the Cybersecurity Examination Program; (iii) conducting IT examinations as part of every FDIC safety and soundness examination of FDIC-insured institutions; and (iv) amplifying cybersecurity threat information as needed. These 2024 activities are discussed in this report.

Examiners

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

As of December 31, 2024, the FDIC employed 2,654 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 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, 2024, the FDIC employed 314 IT examiners, risk management examiners designated as IT Subject Matter Experts, IT Examination Analysts, and Cyber Risk Management Analysts. The total staffing level is substantially the same as the staffing level as of year-end 2023. However, there have been changes in the relative composition of the different categories of examiners, experts, and analysts.

Examiner Education and Instruction

The FDIC, as a member of the FFIEC, participates in the publishing of the *FFIEC Information Technology Examination Handbook* (Handbook).[63] 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

[63] FFIEC, *FFIEC IT Handbook InfoBase*, https://ithandbook.ffiec.gov/.

published the *Architecture, Infrastructure, and Operations (AIO) Booklet*, which sets forth principles and practices for financial institution's management of IT architecture, infrastructure, and operations. More recently, in 2024 the FFIEC published the *Development, Acquisition, and Maintenance Booklet*, which highlights risk management principles and practices for developing, acquiring, or maintaining information technology systems.

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.[64] Recent FFIEC professional development programs addressing cybersecurity and resilience issues included the annual Information Technology (October 2024) and Payment Systems Risk (October 2024) conferences.[65] In addition to the FFIEC programs, the FDIC provides further professional development programs for its supervisory staff, such as the biannual Information Technology and Cybersecurity Summit (March 2025).

In addition, the FDIC's 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 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 cybersecurity threat or vulnerability, such as ransomware threats and supply chain vulnerabilities. In addition, FDIC supervisory staff provide FDIC examiners and other employees with information (in the form of advisories) regarding novel cyber threats and vulnerabilities that may potentially impact FDIC-supervised institutions. While there were no advisories issued to examiners in 2024, over the past four years the FDIC distributed advisories to its examiners on the topics of North Korean infiltration of IT companies, CITRIX bleed, 3CXDesktopApp, and MOVEit file transfer application vulnerabilities.

Examination Work Programs

Examiners use a standardized work program to guide them through examinations of an 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 banking authorities. 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 banking authorities, updated the *InTREx* program to (i) improve the Audit module's usability; (ii) specify compliance review steps relative to the Computer Security Incident Notification Rule; (iii) provide more specificity

[64] FDIC, *Continuing IT Training Program Diagram – Recommended Training Path* (updated February 23, 2023), https://www.fdic.gov/regulations/examiner/it/training_path.html.
[65] FFIEC, Examiner Education Office, https://www.ffiec.gov/exam/courses.html.

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 "horizontal reviews") during a specified period. During 2024, FDIC RMS undertook horizontal reviews on issues related to cyber risk, including (i) significant service providers' consideration of risks associated with developments in quantum computing, and (ii) the effectiveness of the significant service providers' identity and access management controls for privileged accounts.

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 IT 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. 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 interagency efforts to exchange information and publish resources for examining cybersecurity at financial institutions and to provide information to bankers that can be helpful in cybersecurity risk management. For example, the FDIC participates in recurring meetings of the Interagency Intelligence Information Group, which consists of a number of federal financial regulators that share information on common threats to the U.S. financial sector. 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 MOVEit file transfer application vulnerability in 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).[66] 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 to help ensure 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[67] and the Analysis and Resilience Center.[68]

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 2024 and 2025 BCBS efforts to develop updated supervisory principles for financial institutions in the area of third-party risk management, including management of information and cybersecurity risks arising from third-party relationships.

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.[69] 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 revised examples of practices to assist a company in achieving its cybersecurity

[66] Financial Services Sector Coordinating Council, https://fsscc.org/.
[67] Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.
[68] Analysis and Resilience Center, https://systemicrisk.org/.
[69] Press Release, FFIEC, *FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness* (August 28, 2019), https://www.ffiec.gov/press/pr082819.html.

outcome.[70] The FDIC is considering the potential impact of this new version of NIST CSF, and the FDIC may adjust its examination work programs and other cyber-related issuances as appropriate.

Sunset of FFIEC Cybersecurity Assessment Tool (CAT)

In September 2024, the members of the FFIEC issued a statement of the plan to sunset CAT as of August 31, 2025.[71] CAT was originally released by the FFIEC in June 2015 as a voluntary assessment tool to help financial institutions identify their risks and determine their cybersecurity preparedness. The FFIEC statement indicated that, while the fundamental security controls addressed throughout the maturity levels of CAT are sound, several new and updated government and industry resources are available that financial institutions can leverage to better manage cybersecurity risks. These new government resources include the NIST CSF version 2.0 and CISA's Cybersecurity Performance Goals. In October 2024, the FDIC participated in an FFIEC industry outreach webinar regarding the sunsetting of CAT and the path forward for financial institutions to assess their cybersecurity and other related risks using other government and industry resources.

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 institutions have taken steps to address regulatory examination findings and recommendations. At the sector level, recent examples of industry-led efforts include: (i) updates to the Cyber Risk Institute's (CRI) Profile,[72] (ii) continued adoption of the Sheltered Harbor standards and certification process,[73] and (iii) the Global Resilience Federation's Operational Resilience Framework.[74]

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. Over the past four years, there have been several OIG reports issued that relate to the FDIC's supervision of cybersecurity at financial institutions and service providers.

---

[70] National Institute of Standards and Technology (2024) *The NIST Cybersecurity Framework (CSF) 2.0*. (Department of Commerce, Washington, D.C.) *NIST CSWP 29* (February 26, 2024), https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf.
[71] FDIC, Financial Institution Letter No. FIL-61-2024, *Sunset of FFIEC Cybersecurity Assessment Tool* (September 5, 2024), https://www.fdic.gov/news/financial-institution-letters/2024/sunset-ffiec-cybersecurity-assessment-tool.
[72] Press Release, Cyber Risk Institute, *CRI Issues Profile Version 2.1 and Maturity Model – Cyber Risk Institute* (April 15, 2025), https://cyberriskinstitute.org/cri-issues-profile-version-2-1-and-maturity-model/.
[73] Sheltered Harbor, https://www.shelteredharbor.org/.
[74] Press Release, Global Resilience Federation, *The Operational Resilience Framework Introduces New Maturity Model* (November 2, 2023), https://www.grf.org/news/the-operational-resilience-framework-introduces-new-maturity-model.

In 2023, the FDIC OIG released a report on its assessments of the FDIC's efforts to alert supervised institutions of relevant cyber and other threat and vulnerability information.[75] 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 has substantially addressed them.

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)*[76] and *Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program (AUD-23-001)*.[77] The FDIC has addressed the recommendations set forth in these reports.

In addition, on an annual basis, the OIG issues a report setting forth the top management and performance challenges facing the FDIC. In its 2024 report, published in March 2025, the OIG noted that assessing operational resilience in the financial sector was one of the FDIC's top management challenges.[78] In its discussion of this particular challenge, the OIG report stated that "the FDIC faces risks in ensuring that it has examiners with the requisite skillsets to perform IT examinations using existing examination procedures."[79] The OIG report also stated that "it is critical that the FDIC maps the interconnections of banks and their third parties to understand and examine potential operational points of failure and possible cyber intrusion and contagion."[80] As discussed throughout this report, the FDIC continues to use its authorities to mitigate cybersecurity risks in the banking sector.

[75] FDIC Office of Inspector General Report, EVAL-23-002, *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.
[76] FDIC Office of Inspector General Report, AUD-22-003, *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.
[77] FDIC Office of Inspector General Report, AUD-23-001, *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.
[78] FDIC Office of Inspector General Report, *2024 Top Management and Performance Challenges Facing the Federal Deposit Insurance Corporation* (March 2025), https://www.fdicoig.gov/sites/default/files/reports/2025-03/TMPC%20Final%20March%202025.pdf.
[79] Id. at 13.
[80] Id.

THREATS

Tactical

Tactical cybersecurity threats are those that pose risk in the near-term. According to the 14th Annual Ernst & Young (EY)/Institute of International Finance (IIF) Global Bank Risk Management Survey, cybersecurity risk remains the top near-term risk for banks.[81] Furthermore, the International Monetary Fund's 2024 Global Financial Stability Report[82] stated that the number of malicious cyber incidents has increased sharply and that growing digital connectively has likely contributed to the growth in cyber incidents.

Geopolitical events continue to increase the likelihood of cyberattacks on banks. Nation-state affiliated threat groups utilize cyber operations for espionage, destructive attacks, or influence campaigns. Some nation-states have even resorted to using criminal tools and enlisting cybercriminals to facilitate hacking operations.[83] Additionally, some nation-states are increasingly turning to cyber-crime for funding and have deployed ransomware for financial gain and to disrupt critical infrastructure operations of other nation-states.[84]

During 2024, ransomware continued to pose a significant threat to U.S. critical infrastructure sectors, including finance and banking, despite law enforcement takedowns of several ransomware groups in 2024. Extortion attacks involving exfiltration of data along with a threat to publish that data, as well as double extortion attacks which layer on data encryption, were common in 2024. However, some ransomware groups adopted triple extortion tactics which include the additional threat to execute a distributed denial of service attack against the victim or to report the attack to the victim's regulatory authority. Ransomware developers and operators continue to utilize the ransomware-as-a-Service (RaaS) model where affiliates launch attacks developed by operators, making it easier for less technically experienced cybercriminals to launch attacks. Based on a survey of organizations located in a number of different countries, 65 percent of financial service organizations were hit by a ransomware attack in 2024, which percentage-wise was largely unchanged from 2023. Of these attacks, about half were successful in causing a disruption or exfiltrating data. This same survey reported that the mean cost for financial services organizations to recover from a successful ransomware attack rose to $2.58 million.[85] Ransomware can disrupt core business activities, result in operational outages, threaten the confidentiality of customer data, and lead to a loss of customer and counterparty confidence in the financial institution.

Supply chain compromises pose a significant risk to the financial sector as nation-state threat groups and cybercriminals increasingly target software vendors and service providers of

---

[81] Nigel Moden, Tom Campanile & Christopher Woolard, Ernst & Young/Institute of International Finance, *14th Annual EY/IIF Global Risk Management Survey* (February 18, 2025), https://www.ey.com/en_gl/insights/banking-capital-markets/ey-iif-global-bank-risk-management-survey.

[82] International Monetary Fund, *Global Financial Stability Report* (April 9, 2024), https://www.imf.org/en/Publications/GFSR/Issues/2024/04/16/global-financial-stability-report-april-2024?cid=bl-com-SM2024-GFSREA2024001.

[83] Microsoft, *Digital Defense Report 2024* (October 2024), https://www.microsoft.com/en-us/security/security-insider/intelligence-reports/microsoft-digital-defense-report-2024#section-master-oc526b.

[84] Tomar Shloman, Trellix, *Blurring the Lines: How Nation-States and Organized Cybercriminals are Becoming Alike* (January 7, 2025), https://www.trellix.com/blogs/research/blurring-the-lines-how-nation-states-and-cybercriminals-are-becoming-alike/.

[85] Puja Mahendru, Sophos, *The State of Ransomware in Financial Services 2024* (June 24, 2024), https://news.sophos.com/en-us/2024/06/24/the-state-of-ransomware-in-financial-services-2024/.

financial institutions, as these third parties provide a single point of entry that can impact a large number of financial institutions. Security risks arising from compromised third-party 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. According to the Verizon 2024 Data Breach Investigations Report, supply chain attacks were responsible for 15 percent of breaches.[86]

Strategic

Strategic cybersecurity threats are those that are more likely to result in disruptions in the long-term but require current preparation and planning by financial institutions to prevent disruption and add resilience. For example, nation-state threat actors and cybercriminals are leveraging generative artificial intelligence (AI) technologies to research targets, attack vectors and vulnerabilities, as well as to assist with coding malicious software and phishing campaigns.[87] AI is also being used to circumvent financial institutions' identity- and authentication-based network defenses and to perpetrate other frauds on financial institutions and their customers. 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.[88] 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 for financial institutions is the ongoing development of quantum computing technology. Quantum computers use a different computing architecture that can solve certain types of problems, including some encryption algorithms, much faster than traditional computer models. Once fully developed, it is anticipated that quantum computers will provide substantially greater computing speed and power, as compared to current models. A significant strategic risk is that quantum computing is expected to make existing encryption used by financial institutions and other organizations obsolete, thereby enabling malicious actors to decrypt sensitive data. There is also a concern that malicious actors may be harvesting data now in anticipation of being able to decrypt the data in the future using quantum computers. This process is commonly referred to as "harvest now, decrypt later."[89]

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.

[86] Verizon, *2024 Data Breach Investigations Report* (May 1, 2024), https://www.verizon.com/business/resources/reports/dbir/.
[87] Google Threat Intelligence Group, *Adversarial Misuse of Generative AI* (January 29, 2025), https://cloud.google.com/blog/topics/threat-intelligence/adversarial-misuse-generative-ai.
[88] FBI, Public Service Announcement, Alert Number: I-120324-PSA, *Criminals Use Generative Artificial Intelligence to Facilitate Financial Fraud* (December 3, 2024), https://www.ic3.gov/PSA/2024/PSA241203.
[89] National Institute of Standards and Technology, *What Is Post-Quantum Cryptography?* (August 13, 2024, updated *June 11, 2025)*, https://www.nist.gov/cybersecurity/what-post-quantum-cryptography.