# 2023 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) operational 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 FISMA requirements, OMB policy, DHS CISA guidance, and the 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 2022, 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 also reissued a *System Security Authorization Process Guide* to enhance the authorization and continuous monitoring of its information systems and to assist FDIC stakeholders responsible for establishing, operating, and maintaining information security and privacy controls. Key areas of focus in 2022 have included the establishment of a new security and privacy controls catalog with FDIC defined enhancements and parameters, conversion of system security plans, and transition of assessment activities based on new testing guidelines; and improvement of the FDIC Assessment and Authorization Process to begin implementing measures to ensure all FDIC in-house and contractor-managed information systems are subject to the formal authorization process as defined in the Risk Management Framework.

In addition, the FDIC continues to adopt a corporate-wide 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 – 2022,*[5] the auditors concluded that "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 2022 was Level 4 (Managed and Measurable),[6] indicating that the information security program is operating at an effective level of security. In addition, the FDIC has closed nine out of the twelve 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 FISMA Audit report.

The FDIC remains committed to maintaining the security of its systems and protecting sensitive information from unauthorized disclosure. On June 27, 2022, the FDIC updated the FDIC Vulnerability Disclosure Policy[7] consistent with OMB Memorandum M-20-32: *Improving Vulnerability Identification, Management, and Remediation,*[8] and CISA Binding Operational Directive 20-01: *Develop and Publish Vulnerability Disclosure Policy.*[9] This FDIC policy describes the systems and types of security research covered under the policy, to include all of the internet-accessible systems; how to report vulnerabilities; and action for publicly disclosing vulnerabilities.

## Implementation

The FDIC has an established information security program that continues to progress and evolve to meet new challenges. Recently, the FDIC completed actions to strengthen its security controls such as prioritizing the remediation of Plan of Actions and Milestones (POA&Ms); remediating outdated baseline configurations; fully implementing the FDIC's Information Systems Security Management Program; and finalizing an Identity, Credential, and Access Management (ICAM) Roadmap.

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 adoption of cloud services to leverage the flexibility, security, and scalability of cloud technology to meet the urgent challenges of the pandemic such as large IT service demand surges;
- Started an initiative to move the FDIC to a Zero Trust Architecture by submitting a Zero Trust Implementation Plan to OMB, developed a Zero Trust Near Term Strategy, designated an implementation lead, assembled a Core Team and Zero Trust Task Force, and defined a Zero Trust Maturity Model leveraging guidance from the Department of Defense and NIST;

[5] FDIC Office of Inspector General, *The FDIC's Information Security Program – 2022*, September 2022, https://www.fdicoig.gov/sites/default/files/reports/2022-09/AUD-22-004-Redacted.pdf.
[6] CIGIE, *FY 2022 Core IG FISMA Metrics Evaluation Guide*, May 12, 2022, https://www.cisa.gov/sites/default/files/2023-01/fy_2022_core_ig_fisma_metrics_evaluation_guide_05-12-22.pdf.
[7] FDIC, *FDIC Vulnerability Disclosure Policy*, https://www.fdic.gov/policies/vulnerability/.
[8] OMB, M-20-32, *Improving Vulnerability Identification, Management, and Remediation*, September 2, 2020, https://www.whitehouse.gov/wp-content/uploads/2020/09/M-20-32.pdf.
[9] CISA, BOD 20-01, *Develop and Publish a Vulnerability Disclosure Policy*, September 2, 2020, https://www.cisa.gov/news-events/directives/binding-operational-directive-20-01.

- Improved safeguards to protect sensitive information stored in electronic and hard copy format;
- Updated security training to address risks associated with mobile devices and enhance privacy controls;
- Completed an initiative to assess and authorize legacy systems to better align with the NIST Risk Management Framework;
- Conducted Security Control Assessments of cloud-based systems; and
- Enhanced processes to ensure confidentiality agreements for contractor and subcontractor personnel are executed and maintained.

The FDIC's Security Response Team provides centralized technical assistance to effectively investigate and resolve security incidents involving FDIC information. There were 646 security events reported to the CSIRT from October 1, 2021, through September 30, 2022. These security events involved U.S.-based systems and generally had limited impact. None of these events met the criteria for classification as Major incident. During the same period, the FDIC reported 70 of these incidents to the United States Computer Emergency Readiness Team (US-CERT) following the US-CERT Federal Incident Notification Guidelines.[10] All of the incidents reported to US-CERT received a CISA Cyber Incident Scoring System (NCISS) priority score of either Baseline – Negligible or Baseline – Minor.

The EO 14028 on *Improving the Nation's Cybersecurity*[11] issued by President Biden 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. The FDIC has completed all required actions. Additionally, OMB issued Memorandum M-22-09, *Moving the U.S. Government Toward Zero Trust Cybersecurity Principles,*[12] 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.
- Improve Software Supply Chain Security. The EO improves the security of software by requiring the Secretary of Commerce and others to establish baseline security

[10] CISA, *US-CERT Federal Incident Notification Guidelines*, https://www.cisa.gov/sites/default/files/publications/Federal_Incident_Notification_Guidelines.pdf.
[11] 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/.
[12] 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.

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,*[13] 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 has responded 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*,[14] 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*,[15] 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*[16] to provide additional information to aid agencies in

[13] 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.
[14] 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.
[15] 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.
[16] 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.

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*,[17] 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[18] 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*.[19] 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.

OMB issued Memorandum M-23-10, *The Registration and Use of .gov Domains in the Federal Government,*[20] directing 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.[21] The FDIC has responded to all the required actions.

[17] 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.
[18] 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.
[19] 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.
[20] 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.
[21] 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.

The FDIC reported the FY 2022 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, 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 from FY 2022 into FY 2023 issued by CISA:

- ED-22-02: Mitigate Apache Log4J Vulnerability:[22] CISA observed that a series of vulnerabilities in the popular Java-based logging library Log4j were under active exploitation by multiple threat actors. Exploitation of one of these vulnerabilities allows an unauthenticated attacker to remotely execute code on a server. CISA determined that this vulnerability poses an unacceptable risk to Federal Civilian Executive Branch agencies and requires emergency action. The FDIC completed all required actions. CISA closed ED 22-02 and transitioned required actions for Log4J vulnerability to CISA's BOD 22-01: *Reducing the Significant Risk of Known Exploited Vulnerabilities*. BOD 22-01 requires agencies to fully remediate the Log4j vulnerabilities wherever updates are available across all impacted software.
- ED 22-03: Mitigate VMware Vulnerabilities:[23] CISA observed active exploitation by threat actors, including likely advanced persistent threat (APT) actors, of VMware product vulnerabilities. VMware released an update to address these vulnerabilities on April 6, 2022, and the threat actors were able to reverse engineer the update and begin exploitation of impacted VMware products that remained unpatched within 48 hours of the update's release. CISA has determined that these vulnerabilities pose an unacceptable risk to the Federal Civilian Executive Branch (FCEB) agencies and require emergency action. The FDIC completed all required actions.
- BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities:[24] This directive establishes a CISA-managed catalog of known exploited vulnerabilities (KEV) that carry significant risk to federal agencies and establishes requirements for agencies to remediate any such vulnerabilities included in the catalog. This directive enhances but does not replace BOD 19-02, which addresses remediation requirements for critical and high vulnerabilities on internet-facing federal information systems identified through CISA's vulnerability scanning service. The FDIC updated internal

[22] CISA, ED 22-02 (Closed), *Mitigate Apache Log4J Vulnerability*, April 8, 2022, https://www.cisa.gov/news-events/directives/emergency-directive-22-02-closed.
[23] CISA, ED 22-03, *Mitigate VMware Vulnerabilities*, May 18, 2022, https://www.cisa.gov/news-events/directives/emergency-directive-22-03.
[24] CISA, BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, November 3, 2021, https://www.cisa.gov/news-events/directives/binding-operational-directive-22-01.

vulnerability-management procedures in accordance with BOD 22-01 and established a process for ongoing remediation of vulnerabilities that CISA identifies.

- BOD 23-01: Improving Asset Visibility and Vulnerability Detection on Federal Networks:[25] 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[26], 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.

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 1.1[27] 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

[25] 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.
[26] 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.
[27] NIST, *Framework for Improving Critical Infrastructure Cybersecurity, version 1.1*, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.

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 Financial Institutions Examination Council (FFIEC)[28] websites[29] 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.[30] 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,[31] banking organizations, including FDIC-supervised financial institutions, must notify their primary federal regulator of any significant computer-

[28] 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.
[29] 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.
[30] 15 U.S.C. 6801, 6805(b).
[31] 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.

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 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. During the first ten months of the rule's effectiveness (May 1, 2022 through March 31, 2023), the FDIC received seven notifications that met the threshold of the Computer-Security Incident Notification rule.

As a principal member of the Cyber Incident Reporting Council (CIRC),[32] formed in response to the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA),[33] 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 in order to avoid conflicting, duplicative, or burdensome requirements. The FDIC and the other CIRC agencies provided input to a required DHS report that includes: (1) a review of Federal cyber incident reporting requirements; (2) discussion of the challenges to achieve harmonization; (3) proposed actions for DHS; and (4) potential legislation that may be needed to address duplicative reporting. The FDIC is also consulting on a CISA notice of proposed rulemaking that will propose key cyber incident definitions and reporting thresholds.

## 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). For example, in June 2023, the FDIC, FRB, and OCC finalized joint guidance[34] 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-

[32] 6 U.S.C. § 681f.
[33] *Cyber Incident Reporting for Critical Infrastructure Act of 2022*, Public Law No. 117-103 Division Y.
[34] 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.

party relationship. The joint guidance replaces the three agencies' prior guidance on third party risk management.

In August 2021, the FFIEC member entities published guidance on Authentication and Access to Financial Institution Services and Systems,[35] 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. The Guidance includes risk and control considerations for financial institutions when developing an effective authentication program for particular business and risk profiles, such as when multi-factor authentication of users may be an appropriate control to address identified risks.

## 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.[36] 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,[37] 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 January 2022, the FDIC, along with other organizations around the world, learned of potential state-sponsored threats to U.S. critical infrastructure that warranted a heightened state of awareness and a need for organizations to conduct proactive threat hunting to improve their functional resilience. The federal banking agencies shared information and resources from CISA about these state-sponsored threats with all FDIC-insured financial institutions.

[35] 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.
[36] FFIEC, *Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement*, November 3, 2014, https://www.ffiec.gov/press/PDF/FFIEC_Cybersecurity_Statement.pdf.
[37] 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).

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 2022:

- CISA, the National Security Agency, and the Federal Bureau of Investigation Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure advisory (January 14, 2022).
- CISA advisory on information and resources available as part of the U.S. Government's *"Shields-Up"* campaign to promote awareness of current cybersecurity threats and mitigations (February 25, 2022).
- CISA advisory on critical vulnerabilities to unpatched versions of widely used virtualization software that supports cloud computing environments found to be actively exploited by malicious cyber actors (May 19, 2022).

## 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,[38] 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[39] (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).

[38] FDIC, *Directors' Resource Center Technical Assistance Video Program*, https://www.fdic.gov/regulations/resources/director/technical/cybersecurity.html.

[39] 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.

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

- The FDIC issued a *Joint Statement on Heightened Cybersecurity Risk*[40] 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*.[41] 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*,[42] 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*[43] 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.[44] 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 as Treasury drafted the *Financial Services Sector's Adoption of Cloud Services.*[45] This report reflects input from a broad outreach initiative with financial institutions of all sizes, cloud service providers (CSPs), 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

[40] 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.
[41] FFIEC, *FFIEC Issues Statement on Risk Management for Cloud Computing Services*, April 30, 2020, https://www.ffiec.gov/press/pr043020.htm.
[42] FDIC Press Release, *Agencies Release Paper on Operational Resilience*, October 30, 2020, www.fdic.gov/news/press-releases/2020/pr20122.html.
[43] FFIEC, *Cybersecurity Resources Guide for Financial Institutions*, November 2022, https://www.ffiec.gov/press/pdf/FFIECCybersecurityResourceGuide2022ApprovedRev.pdf.
[44] 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.
[45] 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.

services. Recommendations and next steps outlined in the report include CSP tabletop exercises with the financial sector; consideration of operational and cybersecurity threats; policy development relating to system-wide measurement of concentration; and continued engagement internationally through standard setting bodies. In the report, Treasury indicated that it will establish a Cloud Services Steering Group in 2023 that will lead collaboration among U.S. financial regulators, financial sector participants, and CSPs to support the integrity and resilience of cloud-based services (February 8, 2023).

## Outreach

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. Recent examples 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,[46] 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.
- 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 included: Interagency Information Security Standards;[47] IT administrator and security officer independence; cybersecurity preparedness; responding to IT examination matters (e.g., IT governance, privileged user monitoring); and IT risk assessments. In addition, regional outreach programs included discussions on IT due diligence, cybersecurity controls, incident response planning, and computer security incident notification.
- *FDIC and Financial Crimes Enforcement Network (FinCEN) Digital Identity Tech Sprint.*[48] 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).

[46] 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.
[47] 12 C.F.R. § 364.101(b), *Interagency Guidelines Establishing Information Security Standards*.
[48] FDIC Press Release, *FDIC and FinCEN Launch Digital Identity Tech Sprint*, April 5, 2022, https://www.fdic.gov/news/press-releases/2022/pr22030.html.

- *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.*[49] 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).

## 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.[50] Examiners also incorporate the IT rating into the management component of the CAMELS rating.[51] During 2022, the FDIC conducted 1,331 IT examinations at FDIC-supervised institutions and service providers.

Each IT examination results 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[52] to address weak operating practices identified during the examination.

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

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

[49] FDIC, Directors College Program, https://www.fdic.gov/resources/bankers/directors-college-program/index.html.
[50] FFIEC, *Supervision of Technology Service Providers (Appendix A)*, October 2012, https://www.ffiec.gov/press/pr103112.html.
[51] FDIC, RMS Manual of Examination Policies – Basic Examination Concepts and Guideline, March 2022 https://www.fdic.gov/regulations/safety/manual/section1-1.pdf.
[52] FDIC, *FDIC Formal and Informal Enforcement Actions Manual*, https://www.fdic.gov/regulations/examinations/enforcement-actions/index.html.

procedures developed by the FDIC, FRB, and OCC to promote consistent evaluation of this risk.

### 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, 2022, the FDIC employed 2,376 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, 2022, the FDIC employed 305 IT examiners, risk management examiners designated as IT Subject Matter Experts, IT Examination Analysts, and Cyber Risk Management Analysts. This represents a 14.5% decline from year-end 2021 reflecting challenges from external competition for in-demand technology expertise. The FDIC is taking action to address negative staffing trends. For example, the FDIC negotiated a new compensation agreement in 2022 that increased employee pay and benefits.

### Examiner Education and Instruction

The FDIC, as a member of the FFIEC, participates in the publishing of the FFIEC Information Technology Examination Handbook (Handbook).[53] 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 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.[54] Recent FFIEC professional development programs addressing cybersecurity and resilience issues included annual Information Technology (August 2022) and Payment Systems Risk (October 2022) conferences.[55] The FDIC also hosted a biennial Information Technology and Cybersecurity Summit (April 2022) for FDIC examiners that focused on cybersecurity developments, emerging technology issues, and IT-related examination policy with presenters from the FDIC and industry.

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

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 the Apache Log4j compromise, SolarWinds breach, and Microsoft Exchange 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.

The FDIC is updating InTREx with its FRB and state partners to update references, to increase its usability, to provide additional resource assignment flexibility, to update a risk scoring matrix, and to reflect the computer-security incident notification rule. The FDIC is strengthening controls governing use of InTREx examination procedures and work papers; providing staff refresher IT examination training; adopting procedures that ensure threat information supports risk-focused IT examinations; and reviewing the effectiveness of InTREx governance.

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. In 2021 and 2022, the FDIC reviewed ransomware attacks directed at FDIC-supervised institutions and their service providers. Examples of effective controls identified included high-quality multi-factor authentication to control access to systems, and network segmentation that limited the ability of a malicious actor to move laterally in a network. While the FDIC did not identify new categories of controls that needed to be communicated to financial institutions, the review did identify specific controls that made a difference in an institution successfully defending against an attack. The FDIC is now piloting technical examination aids that will help examiners focus on those controls found to be most effective.

### Large and Complex Institution Cyber, IT & Operations Resiliency

In September 2022, the Division of Complex Institution Supervision and Resolution formed the Cyber, Information Technology, & Operational Resilience Section (CITOR). The CITOR Section is responsible for participating in on-site targeted reviews, horizontal examinations, and other supervisory activities to assess the adequacy of

cybersecurity, information technology, and shared services at those FDIC-insured financial institutions with assets greater than $100 billion that are not supervised directly by the FDIC.[56] The CITOR Section also conducts off-site horizontal analysis and risk reporting focused on operational risks that may arise at these large complex financial institutions.

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. This program results in efficient and effective cybersecurity supervision across the largest and most systemically important financial institutions.

### 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 discovered in December 2021 that posed a significant threat to firms across the economy broadly, including financial services. This collaboration resulted in unified communications by the federal banking agencies of urgent information 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).[57] 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

[56] 12 U.S.C. § 1820(a).
[57] Financial Services Sector Coordinating Council, https://fsscc.org/.

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[58] and the Analysis and Resilience Center.[59]

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. Another example of the FDIC's international engagement is collaborating on the September 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.[60] NIST is undertaking a major revision of the CSF through a public-private consultation initiative and states that it plans to publish version 2.0 of the CSF in early 2024.[61] The FDIC is closely following these developments and will adjust examination work programs 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, examples of industry-led efforts include: (1) updates to the Cyber Risk Institute's cybersecurity

[58] Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.
[59] Analysis and Resilience Center, https://systemicrisk.org/.
[60] FFIEC, *FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness*, https://www.ffiec.gov/press/pr082819.html.
[61] NIST, *Updating the NIST Cybersecurity Framework – Journey To CSF 2.0*, https://www.nist.gov/cyberframework/updating-nist-cybersecurity-framework-journey-csf-20.

profile,[62] (2) continued adoption of the Sheltered Harbor standards and certification process,[63] and (3) release of the Global Resilience Federation's Operational Resilience Framework.[64]

### 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 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)*[65] and *Implementation of the FDIC's Information Technology Risk Examination (InTREx) Program (AUD-23-001)*.[66] As detailed in the above Policies and Procedures section of this report, 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.

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.[67] 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 12th Annual Ernst & Young (EY) Global Bank Risk Management survey, cybersecurity risk was the top near-term risk for banks.[68]

---

[62] Cyber Risk Institute, *New CRI Updates Reflect Profile's Ability to Adapt*, January 25, 2023, https://cyberriskinstitute.org/new-cri-updates-reflect-profiles-ability-to-adapt/.
[63] Sheltered Harbor, https://www.shelteredharbor.org/.
[64] Global Resilience Framework, *Operational Resilience Framework v1.0 Released*, November 17, 2022, https://www.grf.org/orf.
[65] 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.
[66] 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.
[67] FDIC, *2022 Annual Report – Appendix 7*, https://www.fdic.gov/about/financial-reports/reports/2022annualreport/ar22section7.pdf.
[68] *12th Annual EY-IIF Bank Risk Management Survey*, January 11, 2023, https://www.iif.com/Publications/ID/5197/12th-Annual-EY-IIF-Bank-Risk-Management-Survey.

Geopolitical events continue to threaten banks that can be targets of related cybersecurity attacks. An increase in malicious activity was attributed to Russia's attempts to damage Ukrainian infrastructure, along with aggressive espionage targeting of Ukraine's allies, including the United States.

Ransomware poses a significant threat to U.S. critical infrastructure sectors, including finance and banking. Ransomware has the potential to disrupt core business activities resulting in operational outages. It can also result in an inability to access critical business and customer data. Malicious actors typically leverage known software vulnerabilities, compromised credentials, and phishing emails targeting financial institution employees 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 model. This makes it easier for less technically savvy cybercriminals to launch attacks.

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 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 Annual Cost of a Data Breach report showed one in five data breaches were due to a software supply chain compromise. A prominent example is the threat of compromise arising from vulnerabilities in Log4J that can allow access to a victimized network's operations and data. The U.S. government warned that the "endemic" script is expected to persist "in the wild" for at least a decade.[69]

An example of a supply chain threat which plagues the banking sector is the compromise by the Russian-based CLOP ransomware group of software used by a managed file transfer service. This ransomware group has also manipulated cloud computing platforms demonstrating an inclination to evolve past well-run compromises on older technologies to more complex technologies. These more modern technologies are sometimes used as 'sandboxes' where the group can refine sophisticated tactics, techniques, and procedures. The availability of these environments where malicious actors can gain knowledge at relatively low cost is expected to grow, making IT network defense increasingly difficult.

### 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 help prevent disruption and add resilience. For example, newer technologies such as ChatGPT and Vall-e are expanding social engineering capabilities allowing novices to create written or audio correspondence (e.g., email or voicemail) with ease that is almost indiscernible from that of trusted persons or sources. The current version of ChatGPT has been shown even to be successful in aiding users to create and refine malware scripts.

Another example is the continuing development of quantum computing technology. While quantum computing promises greater computing speed and power, this technology could be utilized maliciously to compromise modern encryption methods. Financial technologies depend on modern encryption methods. Malicious actors cannot guess passwords and other

[69] Cybersecurity and Infrastructure Security Agency, *Review of the December 2021 Log4j Event*, July 11, 2022, https://www.cisa.gov/sites/default/files/publications/CSRB-Report-on-Log4-July-11-2022_508.pdf.

keys using trial and error because current computing power does not allow them to succeed in a reasonable time. With the release of quantum computing into the public sector, current encryption methods may become inadequate.

## 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.