2022 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 and regulations 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; engages in information sharing and 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 its supervisory programs and strengthen internal operations.

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 National Institute of Standards and Technology (NIST) security standards and guidelines. Of note, FDIC Directive 1310.3, *Information Security Risk Management Program*, defines the FDIC's Information Security Risk Management Program responsibilities with respect to the management of risk to data, and to the information systems and services that use the data in compliance with FISMA and NIST Special Publication 800-37.[4]

In 2021, FDIC developed key policies and procedures impacting essential security control areas including the release of a corporate-wide Supply Chain Risk Management Program directive defining related policies, roles, and responsibilities. The FDIC also issued a *System Security Authorization Process Guide* to improve the authorization and continuous monitoring of its information systems and assist FDIC stakeholders responsible for establishing, operating, and maintaining information security and privacy controls. A key area of the FDIC's focus in 2021 has been integrating the Risk Management Framework (RMF) into business processes, contracts, and projects, and embedding RMF into the Chief Information Officer Organization (CIOO) lifecycle planning and governance processes as those functions take shape. The FDIC has also initiated a multi-year document labeling initiative to identify, categorize, label, and protect FDIC information and data; minimize the risk associated with data leakage; improve information security and data management practices; and facilitate appropriate information sharing.

[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.

In addition, the FDIC continued moving toward 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 FDIC's Information Security Program – 2021*,[5] the auditors concluded "the FDIC established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and NIST security standards and guidelines." The overall FDIC Information Security Program maturity rating for 2021 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 completed actions to address recommendations made in prior-year FISMA audit reports; implemented a process to evaluate and report whether key IT risks were within the FDIC's risk-appetite and established risk-tolerance levels; developed new or revised policies and procedures in key security control areas; completed work on a new backup data center to enhance resiliency; and strengthened monitoring practices to ensure that network users complete required information security and privacy awareness training.

The FDIC remains committed to maintaining the security of its systems and protecting sensitive information from unauthorized disclosure. On March 1, 2021, the FDIC published 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 a Vulnerability Disclosure Policy.*[9] This FDIC policy describes the systems and types of security research covered under the policy, 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. For example, for many years, the FDIC has scanned systems for common vulnerabilities and exposures, used two-factor authentication for access, and provided security awareness training to users, including by conducting phishing exercises designed to reinforce expected behavior. More recently, the FDIC implemented a process to evaluate and report whether key IT risks were within the FDIC's risk appetite and established risk tolerance levels.

[5] FDIC Office of Inspector General, *The FDIC's Information Security Program – 2021*, FDIC Office of Inspector General, October 2021, https://www.fdicoig.gov/sites/default/files/publications/AUD-22-001.pdf.
[6] CISA, *FY2021 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.1*, May 12, 2021, https://www.cisa.gov/sites/default/files/publications/FY%202021%20IG%20FISMA%20Metrics%20Final%20v1.1%202020-05-12.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://cyber.dhs.gov/bod/20-01/.

The FDIC continues to maintain and improve information security consistent with the Cross-Agency Priority goals and FISMA metrics. For example:

- All of the FDIC's mobile devices are operating under enterprise-level mobile device management that includes user authentication requirements and the ability to remotely wipe and remove agency data from the device;
- The FDIC's network is assessed for vulnerabilities by a solution centrally visible at the enterprise level that uses National Vulnerability Database information;
- All privileged users are required to authenticate to the network using a two-factor Personal Identity Verification credential or other Identity Assurance Level 3 / Authenticator Assurance Level 3 credential;
- All endpoints are protected by browser-based and enterprise-based tools to block known phishing websites and Internet Protocol addresses associated with known threats;
- A technology solution is implemented across all of the FDIC's network to detect and alert on the connection of unauthorized hardware assets; and
- The FDIC's network is covered by an automated mechanism to assist in the tracking of security incidents and the collection and analysis of incident information.

The FDIC's Computer Security Incident Response Team (CSIRT) provides centralized technical assistance to effectively investigate and resolve security incidents involving FDIC information. Additionally, CSIRT reports incidents to the U.S. Computer Emergency Readiness Team (US-CERT) following the US-CERT Federal Incident Notification Guidelines.[10] All of the incidents reported to US-CERT from October 1, 2020 to September 30, 2021 received a CISA National Cyber Incident Scoring System[11] priority score of either Baseline – Negligible, or Baseline – Minor.

President Biden signed the EO 14028, "*Improving the Nation's Cybersecurity,*"[12] on May 12, 2021 to support our nation's cybersecurity and protect the critical infrastructure and Federal Government networks underlying our nation's economy and way of life. Recent cybersecurity incidents involving SolarWinds, Microsoft Exchange, and Colonial Pipeline are reminders that the United States' public and private sector entities increasingly face sophisticated malicious cyber activity from both nation-state actors and cyber criminals. The EO 14028 makes a significant contribution toward modernizing our IT and enhancing our cybersecurity defenses. This EO outlines several cybersecurity measures and requirements intended to harden our nation's digital infrastructure against increasingly frequent and sophisticated cyberattacks:

[10] CISA, *US-CERT Federal Incident Notification Guidelines*, https://www.cisa.gov/uscert/incident-notification-guidelines.
[11] CISA, *CISA National Cyber Incident Scoring System*, https://us-cert.cisa.gov/CISA-National-Cyber-Incident-Scoring-System.
[12] EO 14028, *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/.

- Remove Barriers to Threat Information Sharing Between Government and the Private Sector. The EO removes the contractual barriers for IT service providers 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 at-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*,[13] that set a federal zero trust architecture (ZTA) 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 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 program to create an "energy star" type of label so the government, and the public at large, can quickly determine whether software was developed securely. OMB issued Memorandum M-21-30, *Protecting Critical Software Through Enhanced Security Measures*,[14] directing executive departments and agencies to implement the NIST fundamental measures required to secure the use of software in phases. The FDIC has responded to all the required actions.

- Standardize Playbook for Responding to Cybersecurity Vulnerabilities and Incidents. The EO requires the Secretary of Homeland Security and others to create a standardized playbook and set of definitions for cyber vulnerability incident response by federal departments and agencies. The playbook will ensure a more coordinated and centralized cataloging of incidents and tracking of federal agencies' responses. The FDIC will align internal incident response plans and processes with the standardized playbook.

- 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

[13] 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.
[14] OMB, M-21-30, *Protecting Critical Software Through Enhanced Security Measures*, August 10, 2021, https://www.whitehouse.gov/wp-content/uploads/2021/08/M-21-30.pdf.

Government. OMB issued Memorandum M-22-01, *Improving Detection of Cybersecurity Vulnerabilities and Incidents on Federal Government Systems Through Endpoint Detection and Response*,[15] 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 work to 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*,[16] 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. The FDIC has responded to all the required actions.

Furthermore, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*,[17] to significantly change the approach of FISMA oversight and metrics collection by incorporating EO 14028 reporting requirements. The FDIC has responded to all the required actions.

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,

[15] 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.

[16] 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.

[17] 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.

communicate, and manage actions and critical activities related to all directives, in close coordination with OMB.

The FDIC fully complied with the one BOD and five EDs from FY 2021 into FY 2022 issued by DHS:

ED 21-01: Mitigate SolarWinds Orion Code Compromise:[18] SolarWinds Orion products (affected versions are 2019.4 through 2020.2.1.HF1) were exploited by malicious actors. This tactic permits an attacker to gain access to network-traffic management systems. CISA determined that this exploitation of SolarWinds products poses an unacceptable risk to federal agencies and requires emergency actions. The FDIC completed all required actions provided in ED-21-01.[19]

ED 21-02: Mitigate Microsoft Exchange On-Premises Product Vulnerabilities:[20] CISA partners observed active exploitation of vulnerabilities in Microsoft Exchange on-premises products. While the vulnerabilities and exploitative activities are currently not known to have affected Microsoft 365 or Azure Cloud deployments, successful exploitation of these vulnerabilities could allow an attacker to access on-premises Exchange Servers, enabling the attackers to gain persistent system access and control of an enterprise network. CISA has determined that this exploitation of Microsoft Exchange on-premises products poses an unacceptable risk to federal agencies and requires emergency action. The FDIC completed all required actions.

ED 21-03: Mitigate Pulse Connect Secure Product Vulnerabilities:[21] CISA observed active exploitation of vulnerabilities in Pulse Connect Secure products' widely used Secure Sockets Layer remote access solution. Successful exploitation of these vulnerabilities could allow an attacker to place webshells on the appliance to gain persistent system access into the appliance operating the vulnerable software. CISA has no knowledge of other affected Pulse Secure products (including the Pulse Secure Access client). CISA has determined that this exploitation of Pulse Connect Secure products poses an unacceptable risk to federal agencies and requires emergency action. The FDIC completed all required actions and replaced Pulse Connect Secure.

ED 21-04: Mitigate Windows Print Spooler Service Vulnerability:[22] CISA observed the active exploitation of a vulnerability in the Microsoft Windows Print Spooler service. Exploitation of the vulnerability allows an attacker to remotely execute code with system level privileges

[18] CISA, ED 21-01, *Mitigate SolarWinds Orion Code Compromise*, December 13, 2020, https://cyber.dhs.gov/ed/21-01/.
[19] CISA, ED-21-01, Supplemental Direction v4, *Mitigate SolarWinds Orion Code Compromise*, April 22, 2021, https://cyber.dhs.gov/ed/21-01/#supplemental-direction-v4.
[20] CISA, ED 21-02, *Mitigate Microsoft Exchange On-Premises Product Vulnerabilities*, March 3, 2020, https://cyber.dhs.gov/ed/21-02/.
[21] CISA, ED 21-03, *Mitigate Pulse Connect Secure Product Vulnerabilities*, April 20, 2020, https://cyber.dhs.gov/ed/21-03/.
[22] CISA, ED-21-04, *Mitigate Windows Print Spooler Service Vulnerability*, July 13, 2021, https://www.cisa.gov/emergency-directive-21-04.

enabling a threat actor to quickly compromise the entire identity infrastructure of a targeted organization. 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 to mitigate this vulnerability.

ED 22-02: Mitigate Apache Log4J Vulnerability:[23] 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 or Known Exploited Vulnerabilities*. BOD 22-01 requires agencies to fully remediate the Log4j vulnerabilities wherever updates are available across all impacted software.

BOD 22-01: Reducing the Significant Risk of Known Exploited Vulnerabilities:[24] The United States faces persistent and increasingly sophisticated malicious cyber campaigns that threaten the public sector, the private sector, and ultimately the American people's security and privacy. Vulnerabilities that have previously been used to exploit public and private organizations are a frequent attack vector for malicious cyber actors of all types. These vulnerabilities pose significant risk to federal agencies. It is essential to aggressively remediate known exploited vulnerabilities to protect federal information systems and reduce cyber incidents. 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 vulnerability-management procedures in accordance with BOD 22-01 and established a process for ongoing remediation of vulnerabilities that CISA identifies.

FDIC Controls: Over the past year, there continued to be a significant number of high-profile ransomware[25] attacks against corporations, state and local government entities, and non-

[23] CISA, ED 22-02, *Mitigate Apache Log4J Vulnerability*, April 8, 2022, https://www.cisa.gov/emergency-directive-22-02.

[24] CISA, BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, November 3, 2021, https://www.cisa.gov/binding-operational-directive-22-01.

[25] "Ransomware is a type of malicious software that infects and restricts access to a computer until a ransom is paid. Although there are other methods of delivery, ransomware is frequently delivered through phishing emails and exploits unpatched vulnerabilities in software. Phishing emails are crafted to appear as though it has [sic] been sent from a legitimate organization or known individual. These emails often entice users to click on a link or open an attachment containing malicious code." CISA, Ransomware Guidance and Resources, April 11, 2019, https://www.cisa.gov/ransomware.

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[26] 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 the FDIC's actions to strengthen cybersecurity in the financial services sector. The FDIC highlights its policies and procedures relevant to financial sector cybersecurity and resilience along with detail on how the FDIC implements these policies and procedures. This section also discusses the FDIC's efforts to respond to OIG cybersecurity-related findings and recommendations.

Policies and Procedures

The FDIC publishes safety and soundness rules, standards, guidance, and other information to assist FDIC-supervised financial institutions and service providers with establishing effective risk management programs and policies to address cyber-security 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) [27] websites[28] for easy 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. Under Section 39, the FDIC has issued Interagency Guidelines Establishing Standards for Safety and Soundness, which are

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

[27] 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 Office of the Comptroller of the Currency, and the Consumer Financial Protection Bureau, and to make recommendations to promote uniformity in the supervision of financial institutions.

[28] 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.

set forth as Appendix A to Part 364 of the FDIC's Rules and Regulations. These interagency Guidelines apply to all FDIC-supervised financial institutions.

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.[29] These Guidelines set forth standards for financial institutions with respect to 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 bank can build controls effective for the unique risks it faces.

Computer-Security Incident Notification Rule

In November 2021, the federal banking agencies issued a joint final rule to improve the sharing of information by banking organizations regarding computer-security incidents.[30] The final rule requires a banking organization to notify its primary federal regulator of a significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines 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 final 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 final 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. The rule became effective starting May 1, 2022.

Guidance

The FDIC publishes cybersecurity guidance unilaterally and jointly with other regulators. The FDIC coordinates through the FFIEC on much of this guidance. However, in some cases guidance is issued independently by the FDIC 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, the FDIC, FRB, and OCC expect to finalize in 2022 joint guidance[31] to financial institutions regarding the management of risks associated with third-party relationships. This joint guidance

[29] 15 U.S.C. 6801, 6805(b).
[30] 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.
[31] FDIC, Financial Institution Letter No. FIL-50-2021, *Proposed Interagency Guidance on Third-Party Relationships: Risk Management,* July 13, 2021, https://www.fdic.gov/news/financial-institution-letters/2021/fil21050.html.

will set forth principles for a risk management framework to assist financial institutions in managing third-party relationships, including consideration of information security and operational risk associated with third-party relationships. The guidance will take into account the level of function risk, the complexity and size of the financial institution, and the nature of the third-party relationship. The joint guidance will replace each agency's existing 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,[32] 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.

The FDIC collaborated through the FFIEC to issue guidance on several cyber and resilience topics. Notable issuances are:

- *Joint Statement on Destructive Malware* (March 2015);[33]
- *Joint Statement on Cyber Attacks Compromising Credentials (March 2015);*[34]
- *Joint Statement on Cyber Attacks Involving Extortion* (November 2015);[35] and
- *Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs* (April 2018).[36]

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-

[32] 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.
[33] FDIC, Financial Institution Letter No. FIL-13-2021, *FFIEC Joint Statements on Destructive Malware and Compromised Credentials*, March 30, 2015, https://www.fdic.gov/news/financial-institution-letters/2015/fil15013.html.
[34] FFIEC, *FFIEC Releases Two Statements on Compromised Credentials and Destructive Malware*, March 30, 2015, https://www.ffiec.gov/press/PDF/2121758_FINAL_FFIEC%20Credentials.pdf.
[35] FFIEC, *FFIEC Releases Statement on Cyber Attacks Involving Extortion*, November 3, 2015, https://www.ffiec.gov/press/pr110315.htm.
[36] FDIC, Financial Institution Letter No. FIL-16-2018, *FFIEC Issues Joint Statement: Cyber Insurance and Its Potential Role in Risk Management Programs*, April 10, 2018, https://www.fdic.gov/news/financial-institution-letters/2018/fil18016.html.

ISAC) as part of their process to identify, respond to, and mitigate cybersecurity threats and vulnerabilities.[37] 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 primary source from which a financial institution or a service provider could obtain threat information originating from multiple government and private sector sources.

Although financial institutions have other primary sources to obtain information on cybersecurity threats and vulnerabilities, the FDIC, jointly with other financial sector regulatory agencies, amplifies the highest priority communications from U.S. government agencies that track threats and vulnerabilities directly. For example, in early December 2021, the FDIC, along with other organizations around the world, learned of a critical vulnerability in the widely used Apache Log4J logging utility (noted above) that could enable attackers to deploy malicious software or exfiltrate sensitive data. The federal banking agencies shared information and resources from CISA with all FDIC-insured financial institutions to support assessment and mitigation efforts. Given the pervasive nature of this vulnerability, the FDIC also conducted targeted outreach to banks and service providers to sustain heightened awareness to any new information related to the Log4J vulnerability. The FDIC, along with other federal and state regulators, has communicated the following significant alerts and advisories non-publicly to financial institutions since January 2021:

- Update regarding a major supply chain compromise (February 24, 2021);
- Information from CISA on a newly discovered vulnerability in widely used server software (March 5, 2021);
- CISA and FBI best practices advisory for preventing business disruption from ransomware attacks (May 21, 2021);
- CISA, National Security Agency (NSA), and FBI Advisory on Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure (January 14, 2022); and
- 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).

Technical Assistance

The FDIC uses various methods of technical assistance to educate and assist insured depository institutions. The forms of technical assistance include, but are not limited

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

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 cybersecurity and resilience related technical assistance since January 2021 has included:

- Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks.[39] The FDIC, the FRB, and the OCC published a guide to help community banks conduct due diligence when considering relationships with financial technology (fintech) companies. This guide outlines fundamental concepts, including operational resilience considerations, for conducting due diligence on companies that provide new or innovative technologies (August 27, 2021).
- FFIEC Webinar on the Architecture, Infrastructure, and Operations Booklet of the IT Examination Handbook. The FDIC collaborated in the development and delivery of an FFIEC industry webinar to provide an overview of this publication, which is a resource for financial institution examiners when examining the information technology architecture, infrastructure, and operations of a financial institution (November 3, 2021).
- Ransomware Program for Small- to Mid-Size Financial Institutions. The FDIC collaborated with the Financial and Banking Information Infrastructure Committee[40] (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 banking organizations and service providers to address industry questions about computer-security incident reporting (April 28, 2022).

Additional notable cybersecurity- and resilience-related technical assistance programs for financial institutions include:

- The FDIC led development of an FFIEC on-demand webinar for financial institution executives entitled *Executive Leadership of Cybersecurity: What Today's CEOs Need to Know About the Threats They Don't See*. This webinar

[38] FDIC, *Directors' Resource Center Technical Assistance Video Program*, https://www.fdic.gov/regulations/resources/director/technical/cybersecurity.html.
[39] FDIC, Financial Institution Letter No. FIL-59-2021, *Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks*, August 27, 2021, https://www.fdic.gov/news/financial-institution-letters/2021/fil21059.html.
[40] The FBIIC was charted 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.

addressed threats, cyber-risk management, and public/private partnerships like the FS-ISAC that can be helpful in managing cyber-risk (May 7, 2014).[41]

- The FFIEC published observations from cybersecurity assessments of a number of community banks and credit unions, and, as previously noted, recommended that financial institutions of all sizes participate in the FS-ISAC (November 3, 2014).
- In response to the findings of the 2014 cybersecurity assessments, the FFIEC developed and issued the *Cybersecurity Assessment Tool*[42] (Assessment) to help institutions identify risks and determine their level of cybersecurity preparedness. The Assessment provides a repeatable and measurable process for financial institutions to assess cybersecurity preparedness over time. The FFIEC members mapped the Assessment to both the NIST Cybersecurity Framework and the FFIEC IT Examination Handbook to aid institutions in implementation of the tool (June 30, 2015).
- As part of its Community Banking Initiative, the FDIC published cybersecurity resources[43] to encourage discussions of operational risk issues, and the potential impact of IT disruptions on common banking functions. These resources included a Cybersecurity Awareness Directors' College video and three added "Cyber Challenge" exercises, one of which addressed the ransomware scenario. The Cyber Challenge tabletop exercises were first released in 2014 with four operational event vignettes (November 23, 2015).
- The FFIEC published a *Joint Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks*.[44] It reminded financial institutions of the need to actively manage the risks associated with interbank messaging and wholesale payment networks (June 7, 2016).
- The FDIC published two new scenarios in its Cyber Challenge series. The first new scenario provides a flood exercise, and the second a supply chain exercise[45] (October 19, 2018).

[41] FFIEC, *Executive Leadership of Cybersecurity – What Today's CEO Needs to Know About the Threats They Don't See*, May 7, 2014, www.ffiec.gov/press/PDF/CCIWG_Cybersecurity_Draft18forIndustry_May7webinar.pdf.
[42] FFIEC, "Cybersecurity Assessment Tool," June 2015, https://www.ffiec.gov/cyberassessmenttool.htm.
[43] FDIC, Financial Institution Letter No. FIL-55-2015, *Cybersecurity Awareness Resources*, November 23, 2015, https://www.fdic.gov/news/financial-institution-letters/2015/fil15055.html.
[44] FFIEC, *Statement on Cybersecurity of Interbank Messaging and Wholesale Payment Networks*, June 7, 2016, http://www.ffiec.gov/press/PDF/Cybersecurity_of_IMWPN.pdf.
[45] FDIC, Financial Institution Letter No. FIL-63-2018, *Cybersecurity Preparedness Resource*, October 19, 2018, https://www.fdic.gov/news/financial-institution-letters/2018/fil18063.html.

- Along with the other member entities, the FDIC jointly authored the FFIEC *Cybersecurity Resources Guide for Financial Institutions*,[46] which provides a variety of free or low-cost cybersecurity-related resources (October 2018).
- The FDIC issued a *Joint Statement on Heightened Cybersecurity Risk*[47] 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*.[48] 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*,[49] 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).

Outreach

The FDIC also periodically highlights the state of cybersecurity, particular threats and vulnerabilities, and effective controls to mitigate the related risks. Recent examples include:

- FFIEC Webinar on Ransomware Trends. The FFIEC Task Force on Supervision Cybersecurity and Critical Infrastructure Working Group partnered with the U.S. Financial Crimes Enforcement Network to host a webinar on the latest ransomware trends confronting the industry (November 18, 2021).
- FFIEC Webinar on Authentication Guidance. The FDIC collaborated in the development and delivery of an FFIEC outreach webinar to members of the financial services industry to introduce and review the FFIEC Authentication and Access to Financial Institution Services and Systems discussed in the Guidance section of this document (November 3, 2021).
- FFIEC Webinar on Architecture, Infrastructure, and Operations booklet. The FDIC collaborated in the development and delivery of an FFIEC outreach

[46] FFIEC, *Cybersecurity Resources Guide for Financial Institutions*, October 2018, https://www.ffiec.gov/press/pdf/FFIEC%20Cybersecurity%20Resource%20Guide%20for%20Financial%20Institutions.pdf.
[47] FDIC, Financial Institution Letter No. FIL-03-2020, *Joint Statement on Heightened Cybersecurity Risk*, https://www.fdic.gov/news/financial-institution-letters/2020/fil20003a.pdf.
[48] FFIEC, *FFIEC Issues Statement on Risk Management for Cloud Computing Services*, April 30, 2020, https://www.ffiec.gov/press/pr043020.htm.
[49] FDIC Press Release, *Agencies Release Paper on Operational Resilience*, October 30, 2020, www.fdic.gov/news/press-releases/2020/pr20122.html.

webinar to provide an overview of how financial institution examiners assess the risk profile and adequacy of an entity's IT-related architecture, infrastructure and operations activities (November 3, 2021).

- *From Hurricanes to Ransomware: Measuring Resilience in the Banking World*[50] an FDITECH sprint program. The FDIC organized a "tech sprint" on how to foster stronger operational resiliency in the banking system. The program challenged participants to consider existing and proposed measures, data, tools, or other capabilities upon which to build a greater understanding of a bank's resilience to operational hazards. The results of the program support FDIC policymaking efforts (October 2021).
- *FDIC and FinCEN Launch Digital Identity Tech Sprint.*[51] The FDIC in collaboration with the U.S. Treasury Financial Crimes and Enforcement Network organized a "tech sprint" focused on measuring the effectiveness of processes to collect, validate, and verify information about a person that are essential to cybersecurity (January 2022).

Implementation

The FDIC examines IT risk management practices, including cybersecurity, at each FDIC-supervised financial institution as part of the risk management examination. Examiners assign an IT rating using the FFIEC Uniform Rating System for Information Technology (URSIT). Examiners incorporate the IT rating into the management component of the CAMELS rating, in accordance with the FFIEC Uniform Financial Institutions Rating System. During 2021, the FDIC conducted 1,271 IT examinations at state nonmember institutions.

The FDIC's Division of Risk Management Supervision examines the IT operations and systems of FDIC-supervised financial institutions under Section 10 of the FDI Act. The focus of FDIC examinations relative to cybersecurity risk is on the safe and sound operation of the institution's IT systems. The FDIC has promulgated guidelines and regulations in relation to its statutory authority, including Part 364 of the FDIC's Rules and Regulations (discussed above). Moreover, the FDIC may use informal and formal enforcement actions[52] in relation to FDIC-supervised financial institutions to address weak operating practices, deteriorating financial conditions, or other actionable misconduct. The FDIC's formal enforcement decisions and orders are available to the public on the FDIC website[53] and have included IT and information security-related actions.

The FDIC also participates in cybersecurity examinations at the eight U.S. global systemically important banks jointly with the OCC and FRB. The FDIC's Division of Depositor and

[50] FDIC Press Release, *From Hurricanes to Ransomware: Measuring Resilience in the Banking World,* August 16, 2021, www.fdic.gov/news/press-releases/2021/pr21073.html.
[51] FDIC Press Release, *FDIC and FinCEN Launch Digital Identity Tech Sprint*, January 11, 2022, www.fdic.gov/news/press-releases/2022/pr22003.html.
[52] FDIC, *FDIC Formal and Informal Enforcement Actions Manual*, https://www.fdic.gov/regulations/examinations/enforcement-actions/index.html.
[53] FDIC, *FDIC Enforcement Decisions & Orders*, https://orders.fdic.gov/s/.

Consumer Protection examines supervised financial institutions for compliance with privacy-related consumer protection laws and regulations.

The Bank Service Company Act (BSCA) gives the FDIC authority to regulate and examine the performance of bank services provided to supervised financial institutions by third parties, among other provisions. The federal bank regulators frequently examine the performance of such services jointly. In 2021, the bank service provider examination program included a review of service provider controls used to defend against advanced cyber threats, and reviews using cybersecurity examination 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.

As of December 31, 2021, the FDIC employed 2,484 staff in its Division of Risk Management Supervision, the majority of which were examiners. Every commissioned examiner is required to 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 assigns examiners with appropriate 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 management), and IT and Cyber Risk Management Analysts with specialized training and experience in IT and cybersecurity matters. As of December 31, 2021, the FDIC employed 357 IT examiners, risk management examiners designated as IT Subject Matter Experts, IT Examination Analysts, and Cyber Risk Management 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).[54] The Handbook consists of several booklets focused on specific operational risk issues 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.

On June 30, 2021,[55] the FFIEC published the *Architecture, Infrastructure, and Operations* booklet that discusses the interconnections among an entity's assets, processes, and third-party service providers. It also addresses principles and practices for promoting safety and soundness, including secure and resilient architecture

[54] FFIEC, *FFIEC IT Handbook InfoBase*, https://ithandbook.ffiec.gov/.
[55] FFIEC, *Federal Financial Institutions Examination Council Information Technology Examination Handbook on Architecture, Infrastructure, and Operations*, June 2021, https://ithandbook.ffiec.gov/media/402799/ffiec_itbooklet_aio.pdf.

design, infrastructure implementation, and operation of information technology systems.

In addition to the Handbook, the FDIC provides advanced training for examiners who desire to specialize in IT examinations through a formal development program that combines traditional training with coached on-the-job experiences.[56] This program results in participants obtaining an IT subject matter expert credential at the intermediate or advanced levels. Examiners with these credentials examine the more complex banks and service providers, and build the knowledge, skills, and abilities to compete for higher-graded examiner positions.

Finally, from time to time, FDIC subject matter experts provide technical training sessions to examiners that are specific to an exigent threat or vulnerability, such as the Apache Log4j compromise, SolarWinds breach or 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 program, including the examination of cybersecurity and other operational risk-related matters. The FDIC updates this *Information Technology Risk Examination Program (InTREx)* periodically to provide for the continued integrity of IT examination processes and procedures. Changes relate to emerging risks, changes in regulatory guidance, industry trends, and technology developments.

In situations in which the FDIC joins IT examinations conducted by another federal banking agency, the FDIC's examiners use the lead agency's work program.

The federal banking agencies have standardized the work program for examining cybersecurity at the most significant bank service providers. The work program includes cybersecurity examination procedures identified earlier.

Finally, the FDIC creates risk-targeted work programs that examiners use horizontally during examinations at multiple financial institutions or significant service providers. Examples of the focus of these horizontal work programs are interconnections risk and advanced cybersecurity threat risk.

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 ensure the resilience of the U.S.

[56] FDIC, *Continuing IT Training Program*, https://www.fdic.gov/regulations/examiner/it/training_path.html.

financial system. As mentioned previously, the FDIC is active in FFIEC efforts to publish standards 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 was found to pose a significant threat to firms across the economy broadly, including financial services. This resulted in unified communications by the federal banking agencies of urgent information to the industry and examination teams to ensure awareness of the risk, effective mitigation techniques and identify 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] In 2015, the FBIIC and FSSCC jointly created the Financial Services Sector Specific Plan (Plan), which articulates the public/private partnership that exists today. The Plan details 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 that collaborate on initiatives to strengthen the resilience of the financial services sector. The FSSCC is comprised of approximately 70 private sector firms representing financial trade associations, utilities, and major financial services firms. This engagement has resulted in the creation of 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 system.

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 that examinations and other supervisory activities remain relevant.

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 is currently participating in a Basel Committee on Banking Supervision (BCBS) work stream that is considering operational risks, including cyber-risks that may arise from financial institutions' reliance on third party service providers such as cloud service providers. Another

[57] Financial Services Sector Coordinating Council, https://fsscc.org/.
[58] Financial Services Information Sharing and Analysis Center, https://www.fsisac.com/.
[59] Analysis and Resilience Center, https://systemicrisk.org/.

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 that are aligned with widely accepted industry standards.

Industry Response

The financial services industry has taken active steps to prepare for, prevent, and respond to cybersecurity threats, including actions associated with examination findings and recommendations of the regulators. Two examples of industry-led efforts include: (1) the creation of the cybersecurity profile (first by the FSSCC, and now managed by the Cyber Risk Institute),[60] and (2) the creation of the Sheltered Harbor standards and certification process.[61]

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 are relevant to the FDIC's supervision of cybersecurity at financial institutions and service providers.

The OIG released a report in 2020 titled, *The FDIC's Readiness for Crises*.[62] Since its publication, the FDIC has created a Crisis Readiness and Response Section (CRRS) within its Division of Administration, which is responsible for ensuring a holistic, agency-wide approach to emergency readiness and response efforts. Last year, CRRS published an internal directive titled *Crisis Readiness and Response Program,* which established the agency's approach to ensuring readiness and building a coordinated, flexible emergency response system. CRRS has also published an accompanying document, the *Crisis Readiness and Response Framework,* which builds on the directive and provides greater detail on how the FDIC will plan, train, conduct exercises, and organize response teams. CRRS is currently engaged in planning for the government-wide Eagle Horizon continuity exercise, which will feature a cyber-attack affecting federal agencies in the National Capital Region, including the FDIC. Future planning efforts will also update and enhance FDIC plans related to a cyber-incident affecting the financial sector. The FDIC will continue to enhance its readiness plans for specific hazard and threat scenarios, such as a ransomware or other cyber-attack, and in early 2022, the FDIC completed all actions identified in Appendix 6 of the OIG report.

[60] Cyber Risk Institute, https://cyberriskinstitute.org/.
[61] Sheltered Harbor, https://www.shelteredharbor.org/.
[62] FDIC OIG, "The FDIC's Readiness for Crises," April, 2020, https://www.fdicoig.gov/sites/default/files/publications/EVAL-20-004.pdf.

On April 30, 2020, the OIG issued a Management Advisory Memorandum to the FDIC noting the absence of a federal requirement for banks to promptly report instances of disruptive or destructive cyber incidents to Federal banking regulators. Effective May 1, 2022, banks and bank service providers are subject to computer-security incident notification requirements as described above.

In an appendix to the FDIC's 2021 Annual Report,[63] the OIG identified the FDIC's top management challenges. Among those were the "FDIC's Readiness for Crises," and "Cybersecurity for Banks and Third-Party Service Providers." As identified above, the FDIC continues to use its authorities to mitigate cybersecurity risks in the banking sector, and has established new regulatory requirements to ensure third-party service providers share computer-security incident information with bank clients.

Threats

As cybersecurity threats continue to evolve, it is helpful to consider the FDIC's approach to these threats from both a tactical and strategic perspective.

Tactical

Tactical cybersecurity threats are those requiring an operational response because they may lead to actual incidents. For example, the threat of a successful ransomware attack that disrupts a bank's or service provider's core services or critical business lines has evolved into a growing number of actual incidents. The use of ransomware to extort illicit payments continues to be a significant risk to the financial sector. In February 2022, CISA and the NSA issued a joint alert titled, *2021 Trends Show Increased Globalized Threat of Ransomware,*[64] which stated that ransomware attacks grew and evolved in 2021. The alert highlighted that cybersecurity authorities in the United States, Australia, and the United Kingdom observed an increase in sophisticated, high-impact ransomware incidents against critical infrastructure organizations globally. There is no indication that the elevated levels of operational risk from threats such as ransomware in the banking sector will abate in the near term. Moreover, the proliferation of tactics and tools made available by experienced malicious cyber actors through "ransomware-as-a-service" offerings have made it easier for a growing number of unsophisticated recruits to target a greater number of business of all types including financial services. Further, outside of developing new ransomware campaigns, the growing professionalization of this "dark market" has led to more effective versions of ransomware.

Another example of a tactical threat is that malicious cyber threat actors seek to gain access to bank information systems by compromising the security of software and computing services provided by third-party suppliers. A bank's IT environment is a complex arrangement of self-developed software, third-party software hosted internally, and third-party software accessed remotely, such as cloud-based software services. Malicious actors have sought to

[63] FDIC, *2021 Annual Report – Appendix 7*, https://www.fdic.gov/about/financial-reports/reports/2021annualreport/ar21section7.pdf

[64] CISA, Alert AA22-040a, *2021 Trends Show Increased Globalized Threat of Ransomware*, February 9, 2022, https://www.cisa.gov/uscert/ncas/alerts/aa22-040a.

gain access to bank IT systems by inserting malicious software into third-party software during its development, and by leveraging undiscovered vulnerabilities in the third-party software. The security risks arising from compromised third-party software are challenging to mitigate given the multitude of third-party software within a bank's IT environment, and the sophistication of some of the software compromises. In addition, these third-party software and computing services supply chain attacks have the potential to negatively affect the security and operations of a bank as attackers increasingly target third-party software that controls privileged access and roles within the bank's IT environment, such as network management and security software applications.

The 2021 SolarWinds and Kaseya VSA attacks, both of which prompted changes in supply chain protocols and guidelines for the U.S. government and commercial industries, highlighted the supply chain's vulnerability to cyber-attacks. Evidence suggesting that state-sponsored cyber actors may have participated in these attacks has intensified the urgency to address supply chain vulnerabilities. These threats are expected to continue in 2022 and beyond.

Strategic

Strategic cybersecurity threats may not have yet resulted in incidents, but require ongoing preparedness and planning to help prevent disruption and add resilience to IT systems. For example, recent geopolitical events have increased the likelihood of cyber-attacks on the financial sector. In the first quarter of 2022, CISA issued multiple alerts addressing Russian state-sponsored cyber threats and highlighting recent malicious cyber incidents suffered by public and private entities in Ukraine. Given ongoing geopolitical events, CISA issued alerts addressing risks from Russian State-Sponsored cyber threats[65] and highlighted recent malicious cyber incidents suffered by public and private entities in Ukraine.[66] CISA, the FBI, and the NSA encourage organizations of all sizes to adopt a heightened state of awareness and to be prepared to respond to disruptive cyber activity.

Another example of a strategic threat is the continuing development of quantum computing technology that can be leveraged to break current encryption technology. Industry and the U.S. government are working to address this threat in multiple ways. For example, NIST has initiated a process to solicit, evaluate, and standardize one or more quantum-resistant public-key cryptographic algorithms.[67] To make the financial services industry aware, quantum research experts have briefed private and public sector attendees at multiple financial

[65] CISA, Alert AA22-011A, *Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure*, January 11, 2022, https://www.cisa.gov/uscert/sites/default/files/publications/AA22-011A_Joint_CSA_Understanding_and_Mitigating%20_Russian_Cyber_Threats_to_US_Critical_Infrastructure_TLP-WHITE_01-10-22_v1.pdf.

[66] CISA, *Implement Cybersecurity Measures Now to Protect Against Potential Critical Threats*, January 18, 2022, https://www.cisa.gov/sites/default/files/publications/CISA_Insights-Implement_Cybersecurity_Measures_Now_to_Protect_Against_Critical_Threats_508C.pdf.

[67] NIST, Computer Security Resource Center, *Post-Quantum Cryptography*, https://csrc.nist.gov/projects/post-quantum-cryptography.

services sector meetings on the threat to the confidentiality of stolen sensitive information that is encrypted with current commercial encryption techniques.

Conclusion

The cybersecurity threat remains significant, and is continually evolving. The FDIC will continue to use its authorities to battle this threat creatively, and in partnership with other private and public sector stakeholders.