



REPORT TO CONGRESS

Cybersecurity and Financial System Resilience Report



September 2026

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM



The Federal Reserve is the central bank of the United States. It performs five key functions to promote the effective operation of the U.S. economy and, more generally, the public interest.

The Federal Reserve

- **conducts the nation's monetary policy** to promote maximum employment and stable prices in the U.S. economy;
- **promotes the stability of the financial system** and seeks to minimize and contain systemic risks through active monitoring and engagement in the U.S. and abroad;
- **promotes the safety and soundness of individual financial institutions** and monitors their impact on the financial system as a whole;
- **fosters payment and settlement system safety and efficiency** through services to the banking industry and U.S. government that facilitate U.S.-dollar transactions and payments; and
- **promotes consumer protection and community development** through consumer-focused supervision and examination, research and analysis of emerging consumer issues and trends, community economic development activities, and administration of consumer laws and regulations.

To learn more about us, visit www.federalreserve.gov/aboutthefed.htm.

Contents

Overview	1
Board Policies and Procedures for Cybersecurity Risk Management	3
Board Supervisory Policies and Procedures	3
Board Internal Policies and Procedures	4
Board Activities to Address Cybersecurity Risks	7
Supervisory Activities	7
Board Internal	18
Current or Emerging Threats to Financial System Resilience	21
Artificial Intelligence	21
Geopolitical Tensions	22
Cyber-Criminal Activity	22
Cybersecurity Risks Associated with Third-Party Providers	23
Emerging Quantum-Related Risks	25

Overview

The Consolidated Appropriations Act, 2021¹ (CAA) requires the Board of Governors of the Federal Reserve System (Board) to submit annually for seven years a report focused on cybersecurity to Congress. The CAA calls for a description of measures the Board has undertaken to strengthen cybersecurity within the financial services sector and with respect to the Board's functions as a regulator, including the supervision and regulation of financial institutions and third-party service providers. Pursuant to the CAA, this report is organized in three main sections covering:

- [the Board's policies and procedures](#) related to cybersecurity risk management, including with respect to the Board's supervision and regulation of financial institutions, the Board's administration of its internal information security program, and the Reserve Banks' information security program;
- [Board activities to address cybersecurity risks](#), including those carried out through our supervision of financial institutions, through the Board's own programs and initiatives, and through those of the Reserve Banks as a provider of critical payment and settlement services; and
- [current or emerging cybersecurity threats](#) that may pose a risk to the resilience of the financial system.

As described in the report, the Board views cybersecurity as a high priority for the Federal Reserve System (System) and Board-supervised institutions. The Board and the Reserve Banks maintain and continuously improve information security programs and engage and coordinate on cybersecurity issues with numerous critical stakeholders including the financial regulatory agencies and industry. These efforts include actively monitoring cybersecurity threats and responding, as appropriate, to incidents that could affect the operations of the Board, the Reserve Banks, or Board-supervised institutions.

¹ Consolidated Appropriations Act, Pub. L. No. 116-260, Division Q, section 108 (2021).

Board Policies and Procedures for Cybersecurity Risk Management

The Board recognizes the increasing and evolving nature of cybersecurity threats to the financial system. Accordingly, the Board's supervision and regulation of financial institutions encompasses review and monitoring of institutions' cybersecurity risk management and information technology (IT) programs. As part of its safety and soundness supervision, the Board issues cybersecurity-related regulations, guidance, tools, and resources; examines and monitors supervised institutions' cybersecurity risk-management posture; and collects data on cybersecurity incidents (along with the other federal financial regulatory agencies) to monitor trends in the financial sector. Additionally, the Board and the Reserve Banks secure their internal information and information systems through robust cybersecurity risk-management programs. The Board follows the Federal Information Security Modernization Act (FISMA) requirements, and the Reserve Banks also employ a framework based on the National Institute of Standards and Technology's (NIST) standards and guidance.

Board Supervisory Policies and Procedures

The Board's supervisory policies and examination procedures are aimed at reducing the risk of cybersecurity threats to the financial system through effective cybersecurity practices at supervised institutions. The Board issues and publishes rules, guidance, tools, and resources for supervised institutions regarding IT risk management, cybersecurity, operational resilience, third-party risk management, and other related topics.²

The Board, along with other federal regulators, issued the Interagency Guidelines Establishing Information Security Standards, which require banking organizations to develop and implement administrative, technical, and physical safeguards to promote the security, confidentiality, and integrity of customer information.³ The guidelines require banks to have internal controls and information systems appropriate to the size of the institution and the nature, scope, and risk of its activities. Other requirements include having effective risk management, adequate procedures to safeguard and manage assets, and internal audit systems that provide for adequate testing and review of information systems. The Board also issues guidance on these topics and provides

² See Board of Governors of the Federal Reserve System, "Information Technology Guidance," last modified February 4, 2022, <https://www.federalreserve.gov/supervisionreg/topics/information-technology-guidance.htm> and Board of Governors of the Federal Reserve System, "Operational Resilience," last modified February 4, 2022, <https://www.federalreserve.gov/supervisionreg/topics/operational-resilience.htm>.

³ See 12 CFR pt. 208, appendix D-2; 12 CFR pt. 225, appendix F. These requirements of banking organizations are promulgated pursuant to title V, subtitle A, of the Gramm-Leach-Bliley Act.

resources and tools that financial institutions may use to build upon existing cybersecurity practices.

Recently, the Board released a statement on supervisory operating principles describing broad changes to strengthen supervision by focusing on identifying and taking proportionate action as early as possible to eliminate the most important risks threatening the safety and soundness of banking organizations.⁴ Among other things, these principles direct Federal Reserve examiners to rely to the maximum extent possible on the examinations and other supervisory work by the primary state or federal banking supervisor; to tailor their supervision based on the size, complexity, and systemic importance of a particular banking organization; and to prioritize attention on material financial risk. Recognizing that cyber incidents have the potential to contribute significantly to material financial risk, cybersecurity remains a top priority for the Federal Reserve and our approach to supervision.

Board Internal Policies and Procedures

The Board continues to take a proactive approach to safeguarding its operations and assets by developing, documenting, and implementing a comprehensive security program. The program is designed to protect both the information and information systems that support the agency's core mission and functions. The Board's information security program follows federal information security requirements as established by FISMA and related NIST standards.

The Board is taking steps to further improve its security posture by implementing the latest cybersecurity standards and principles. One key area of focus is the adoption of zero-trust principles,⁵ which has further enhanced the Board's cybersecurity posture by requiring users to continuously verify credentials when using internal resources. A second area of focus is supply chain risk management (SCRM), which will ensure Board information and services remain secure even as we leverage third parties to store and process our information. Furthermore, the Board also collaborates with cybersecurity consultants and experts, who provide independent recommendations on improving the Board's cybersecurity controls and protocols.

In addition to administering the agency's information security program, the Board also oversees the cybersecurity risk-management posture of the Reserve Banks. The Reserve Banks have a comprehensive, risk-based information security program that is informed by NIST standards and

⁴ See Statement by Mary Aiken and Julie Williams, "Statement of Supervisory Operating Principles," press release, October 29, 2025, <https://www.federalreserve.gov/newsevents/pressreleases/files/bcreg20251118a1.pdf>. This announcement was superseded by a statement released in 2026. See Statement by Randall D. Guynn and Julie Williams, "Updated Statement of Supervisory Operating Principles," press release, April 21, 2026, <https://www.federalreserve.gov/supervisionreg/files/statement-of-supervisory-operating-principles-20260430.pdf>.

⁵ See 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>.

guidance and industry best practices. The Reserve Banks, as operators of critical financial services, proactively provide tools and communications aimed at mitigating cybersecurity risks to their financial institution customers. Additionally, Federal Reserve Operating Circular No. 5, Electronic Access, sets forth the information security requirements applicable to institutions accessing Reserve Bank services, such as the Fedwire Funds Service, Fedwire Securities Service, FedACH, FedNow Service, and National Settlement Service.⁶ Under Operating Circular No. 5, institutions are required to implement technical, operational, managerial, and procedural controls designed to protect the security of the IT environment, including systems and processes that are used to access Reserve Bank services and applications.

⁶ See “Federal Reserve Banks Operating Circular No. 5 Electronic Access,” effective May 1, 2024, <https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/050124-operating-circular-5.pdf>.

Board Activities to Address Cybersecurity Risks

The Board's activities help confirm that policies, procedures, rules, and guidance for supervised institutions and internal agency functions are successfully implemented. The Board's approach includes providing appropriate cybersecurity-related staffing, training, and resources for bank examiners. The Board's Office of Inspector General (OIG) also conducts independent reviews of the Board's focus to continually improving cybersecurity supervisory activities and enhancing internal processes. The Board's activities involve interagency, intergovernmental, industry, and international collaboration.

Supervisory Activities

The Federal Reserve conducts examinations and monitoring of cybersecurity risk management, governance, and controls at supervised institutions. It also examines and monitors, pursuant to the Board's authority under the Bank Service Company Act (BSCA),⁷ certain services performed on behalf of financial institutions by their service providers. The Federal Reserve's supervision activities in this area promote financial institutions' ability to protect against cybersecurity incidents and other hazards, safeguard critical infrastructure, and address emerging technology risks. Federal Reserve examination staff use the Uniform Rating System for Information Technology (URSIT) and the Federal Financial Institutions Examination Council (FFIEC)⁸ IT Handbook, which is informed by NIST standards and guidance along with other sources, in conducting cybersecurity and other information technology-related examinations.⁹

Examiners evaluate cybersecurity with consideration of the business models and activities conducted by supervised institutions as part of a principles-based supervision program. In addition to these considerations, the scope of any specific examination also considers key cybersecurity risks, the industry landscape, and other factors such as emerging technologies. As part of these evaluations, examiners consider business-line controls, risk-management practices, assurance functions, and governance activities performed by the firm's senior management and board of directors.

For the eight U.S. global systemically important banks, the Federal Reserve conducts joint cybersecurity examinations with the Office of the Comptroller of the Currency (OCC) and Federal Deposit Insurance

⁷ 12 U.S.C. §§ 1861-67.

⁸ See website for membership, <https://www.ffiec.gov/about/leadership-staff>.

⁹ See Federal Financial Institutions Examination Council, "FFIEC Information Technology Examination Handbook Infobase," <https://ithandbook.ffiec.gov/>.

Corporation (FDIC). Additionally, for large financial institutions with assets of \$100 billion or more,¹⁰ the Federal Reserve conducts common scope cybersecurity examinations across several institutions at once. Common scope examinations provide more consistency in the assessment of cybersecurity risk management across firms, identify the range of practices observed at firms, and, as appropriate, allow the Federal Reserve to issue supervisory findings. Supervised findings are issued when identified cybersecurity deficiencies result in a violation of regulation, impact the safety and soundness of a supervised firm, or threaten the U.S.'s financial stability. In addition to common scope reviews, supervisory teams monitor cybersecurity, IT, and operational risk using continuous monitoring processes as well as monthly engagement focused on emerging threats.

For state member community banking organizations (those with under \$10 billion in assets) and regional banking organizations (those with \$10 to \$100 billion in assets), URSIT is the primary mechanism to inform evaluations of cybersecurity practices and assign IT ratings to each firm. If deficiencies in an institution's cybersecurity program are identified, examiners may issue supervisory findings. Firms are expected to promptly address findings to ensure appropriate protection against cybersecurity threats.

For community banking organizations and regional banking organizations, the Board follows a risk-focused approach that assigns examination resources to higher-risk banks and areas of each bank's operations and encourages banks to maintain risk-management capabilities appropriate to their size and complexity. Cybersecurity practices are evaluated through regular IT examinations. For state member banks, these examinations are often conducted jointly with state banking regulators. The Federal Reserve along with the FDIC and state banking authorities use the Information Technology Risk Examination Program (InTREx), which provides supervisory staff with risk-focused and efficient examination procedures for assessing IT and cybersecurity risks at supervised institutions. InTREx procedures may also be used in conjunction with those listed in the FFIEC IT Handbook¹¹ when a financial institution's risk or complexity is elevated.

The Federal Reserve expects the financial institutions it oversees to effectively manage risks associated with their third-party service providers. Additionally, the BSCA provides authority for the federal banking agencies (FBAs)¹² to regulate and examine certain services performed by third parties on behalf of insured depository institutions and their affiliates. The FBAs jointly supervise a subset of third-party technology service providers through an interagency technology service

¹⁰ Banking organizations posing the greatest risk to U.S.'s economic and financial system are supervised by the Global Systemically Important Banks (GSIBs) program (previously called the Large Institution Supervision Coordination Committee (LISCC) program). GSIBs are the largest and most complex banking organizations headquartered in the U.S. Current G-SIB firms are Bank of America Corporation; The Bank of New York Mellon Corporation; Citigroup, Inc.; The Goldman Sachs Group, Inc.; JPMorgan Chase & Co.; Morgan Stanley; State Street Corporation; and Wells Fargo & Company. A Large and Foreign Banking Organization (LFBO) firm refers to a domestic or foreign banking organization with combined U.S. assets of \$100 billion or more that is supervised under the LFBO supervisory program.

¹¹ See Federal Financial Institutions Examination Council, "FFIEC Information Technology Examination."

¹² The federal banking agencies are the Board, OCC, and FDIC.

provider supervision program, which incorporates a risk-based process for selecting service providers for inclusion in the program. Through examinations of service providers in the program, the FBAs issue an URSIT rating evaluating each service provider. As part of the examination program, the FBAs conduct cybersecurity-specific examinations of these service providers which inform their overall URSIT rating. They issue reports of examination, communicate supervisory findings, and take enforcement actions when needed. The report of examination is distributed on a confidential basis to the service provider and to the provider's client financial institutions to assist with their ongoing monitoring of third-party risk.

In addition, the Federal Reserve's consumer compliance supervision program complements the IT and cybersecurity reviews conducted by safety and soundness examiners to ensure that supervised institutions maintain systems and processes to protect customers' sensitive personal financial information. Through this program, the Federal Reserve's examiners evaluate the effectiveness of supervised institutions' compliance with consumer financial privacy laws and regulations.¹³

With regard to financial market utilities (FMUs), the Board has direct supervisory authority for a subset of the FMUs designated by the Financial Stability Oversight Council (FSOC). The Board also works closely with staff at the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC), to oversee the other designated FMUs supervised by those agencies, as permitted by title VIII of the Dodd-Frank Wall Street Reform and Consumer Protection Act (Dodd-Frank Act).¹⁴ The Board has set expectations for FMUs' operational and cybersecurity risk-management programs in Regulation HH (Financial Market Utilities).¹⁵ The Board regularly sets supervisory priorities for and examines (or participates in CFTC- and SEC-led examinations of) designated FMUs' operational risk-management frameworks.¹⁶ The Board also reviews proposed changes to designated FMUs' rules, procedures, and operations, including proposed changes that would materially affect a designated FMU's management of operational and cybersecurity risk.

The Federal Reserve uses the Organization; Risk Management; Settlement; Operational Risk and Information Technology; and Market Support, Access, and Transparency (ORSOM) rating system in its assessment of designated FMUs for which the Board is the supervisory agency under title VIII of the Dodd-Frank Act. The rating system facilitates discussion of the FMU's condition with the

¹³ Examples include Regulation P (12 CFR pt. 1016.) and the "red flags" rule under the Fair Credit Reporting Act (15 U.S.C. § 1681m(e)).

¹⁴ See Board of Governors of the Federal Reserve System, "Designated Financial Market Utilities," last modified January 29, 2015, https://www.federalreserve.gov/paymentsystems/designated_fmu_about.htm.

¹⁵ See Financial Market Utilities, 79 Fed. Reg. 3666 (April 15, 2024), <https://www.federalregister.gov/documents/2024/03/15/2024-05322/financial-market-utilities>.

¹⁶ Under section 807(d) of the Dodd-Frank Act, the Board may, at its discretion, participate in any title VIII examination led by the SEC or CFTC. 12 U.S.C. § 5466(d)(2).

FMU's management and board of directors. Supervisory staff explain to the FMU the factors that determine the FMU's rating, including operational, IT, and cybersecurity risks.¹⁷

The Federal Reserve has established processes and programs to monitor and share information involving cybersecurity threats, vulnerabilities, and incidents. Additionally, the Federal Reserve monitors cybersecurity developments and events across the financial services sector, including payment, clearing, and settlement systems. The Federal Reserve proactively educates examination staff on cybersecurity threats or vulnerabilities. This helps examination staff to evaluate risks to supervised institutions and inform supervisory engagement.

Incident Response Efforts

The Federal Reserve's supervisory incident response processes enable an effective and repeatable supervisory response to cybersecurity incidents that affect Federal Reserve-supervised institutions and service providers. The FBAs receive notifications from banking organizations about computer-security incidents that may affect the U.S. banking system, as required under the Computer-Security Incident Notification Rule, promulgated in 2021.¹⁸ The rule requires a banking organization to notify its primary federal regulator of any significant computer-security incident as soon as possible and no later than 36 hours after the banking organization determines that a notification incident has occurred. Bank service providers are required to notify affected banking organization customers as soon as possible regarding certain computer-security incidents so the customer banking organizations can determine whether a notification incident has occurred. The notifications help the agencies become aware of and react to emerging threats and incidents.

Under Regulation HH, a designated FMU for which the Board is the supervisory agency is required to immediately notify the Board of material operational incidents. Additionally, Regulation HH requires a designated FMU to establish criteria and processes for providing timely communication and responsible disclosure, such that it provides (1) immediate notice to affected participants in the event of actual disruptions or material degradation to its critical operations or services or to its ability to fulfill its obligations on time and (2) timely notice to participants and other relevant entities of all other material operational incidents that require immediate notification to the Board, taking into account the risks and benefits of disclosure to the designated FMU and to participants and other relevant entities.¹⁹

¹⁷ For designated FMUs that are primarily supervised by the CFTC or SEC, Federal Reserve supervisory staff communicate views of the FMU's cyber-risk management to the CFTC or SEC, as appropriate.

¹⁸ See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (April 1, 2022), <https://www.federalregister.gov/documents/2021/11/23/2021-25510/computer-security-incident-notification-requirements-for-banking-organizations-and-their-bank>.

¹⁹ See 12 CFR pt. 234.

Cybersecurity-Related Findings

As part of the Board's safety and soundness supervision, Federal Reserve supervisors examine and monitor the information security practices and cybersecurity programs of supervised institutions and may issue supervisory findings notifying supervised institutions of identified deficiencies. The Federal Reserve requires supervised institutions to respond appropriately to cybersecurity-related supervisory findings and take proactive steps to mitigate cybersecurity risks. When institutions do not address findings in an appropriate period of time, the Board has tools such as informal and formal enforcement actions to ensure institutions operate in a safe and sound manner.

Staffing, Training, and Deployment of Examiner Resources

The Federal Reserve maintains an experienced, trained complement of supervision staff with IT expertise, including individuals with expertise in cybersecurity. Federal Reserve examiners assess supervised institutions' cybersecurity and information security practices, internal audit, risk management, and controls to ensure that institutions implement appropriate and effective safeguards to mitigate cybersecurity risk. For large domestic firms and service providers, examiners are assigned to a specific firm or group of firms using a risk-based approach, and for foreign entities and smaller domestic institutions, examiners are assigned on a portfolio basis.

The Federal Reserve has established frameworks to guide the recruitment and assignment of examiners, including IT and cybersecurity risk specialists. The Federal Reserve coordinates and conducts training and makes available to staff a learning platform with an extensive catalogue of cybersecurity, IT, and information security training. We also leverage conferences and training hosted by the FFIEC and government agencies. In addition, Federal Reserve examiners participate in training events to gain perspective from external cybersecurity practitioners and industry experts. Federal Reserve staff collaborate to share information and institutional knowledge of cybersecurity resilience issues, and to address operational resilience matters across the portfolios supervised by the Federal Reserve. The Federal Reserve continues to assess and offer cybersecurity skills training aligned with risks to supervised institutions.

Board OIG Efforts Related to Supervisory Activities

On February 3, 2026, the OIG issued the report, *Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS*.²⁰ The report identified one finding and made four recommendations, which focus on implementing need-to-know principles for Federal Reserve System user access, developing portfolio-specific access approaches, updating guidance on sensitive file folders, and establishing clear access review

²⁰ See Board of Governors of the Federal Reserve System, Office of Inspector General, *Results of Scoping of the Evaluation of the Board's Practices and Controls for Safeguarding Confidential Supervisory Information in OASIS* (Board of Governors, February 2026), <https://oig.federalreserve.gov/reports/board-confidential-supervisory-information-feb2026.htm>.

procedures. The Board submitted a management response and is executing a plan to address the recommendations.

On May 28, 2025, the OIG issued the report, *The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations (CBO)*.²¹ The report identified findings and made five recommendations related to the Board's work programs and training for CBO IT examinations. The Board reviewed the report and is addressing these recommendations.

Reserve Bank Activities

In addition to managing its internal cybersecurity program, the Board also supervises the 12 Reserve Banks' IT and information security operations and oversees the implementation and ongoing management of cybersecurity across the System. Given the scale, severity, and increasing frequency of cyberattacks, the Reserve Banks recognize that a significant incident within their environment can have a severe impact on the economy and undermine the integrity and stability of the financial sector. In response to these heightened risks to the Reserve Banks, the System remains steadfast in its commitment to strengthening the cybersecurity posture by prioritizing initiatives and collaboration by continually conducting cybersecurity risk assessments and mitigations, proactively monitoring and improving recovery capabilities by building resilient systems.

In 2025, the Federal Reserve strengthened its security posture through several strategic initiatives. These included creating robust artificial intelligence (AI) deployment protocols and maturing its identity and access management capabilities. The Federal Reserve also accelerated efforts to modernize their encryption capabilities to remain effective against future quantum computing risks. Collectively, these efforts strengthened its cybersecurity infrastructure against evolving threats in the financial sector. These accomplishments reflect the Reserve Banks' ongoing dedication to collaborating with the public and private sector to further improve the overall state of information security across the System.

The Reserve Banks, as in prior years, continued to focus on strengthening the security of the U.S. payment system, which includes fortifying and optimizing the cybersecurity posture and operational resilience of the suite of payment applications operated by the Federal Reserve Financial Services. This includes enhancing the resilience and recovery capabilities of its payment platforms. The approach involves rigorous testing using a comprehensive set of varied cybersecurity scenarios that simulate real-world risks. At the same time, it evaluates the potential business impacts on both the Federal Reserve and its customers (e.g., service disruptions or transaction delays). These enhancements are intended to ensure swift resumption of critical operations with

²¹ See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board Can Enhance Its Approach to the Cybersecurity Supervision of Community Banking Organizations* (Board of Governors, May 2025), <https://oig.federalreserve.gov/reports/board-cybersecurity-community-banking-may2025.htm>.

minimal business impact during local, regional, or widespread disruptions, and to implement sound measures to safeguard data integrity throughout the process. The Federal Reserve also educates depository institutions that connect to our payment system on cybersecurity risks and works with them during individual and sector-wide cybersecurity events.

Finally, the Board stays abreast of the enacted federal laws on cybersecurity and executive orders focused on cybersecurity and resiliency to ensure Systemwide compliance. The Reserve Banks collaborate closely with one another and are able to forge strategic relationships with government partners to further enhance the state of information security and resiliency across the System.

Coordination Activities

Due to the high degree of interconnectedness of the global financial system, the Board remains engaged in domestic and international forums addressing the cybersecurity resiliency of the financial sector. Board and System staff work together to coordinate with other domestic and international agencies, governance bodies, financial regulators, and industry to share information and best practices as well as publish guidance for regulated entities.

Intergovernmental Coordination

To strengthen risk-management practices across the financial sector and reduce the effects of cybersecurity-related incidents, the Board coordinates with partners through the President's Working Group on Financial Markets (PWGFM), the Financial Stability Oversight Council (FSOC), the Financial and Banking Information Infrastructure Committee (FBIIC), and the FFIEC.

The PWGFM was established to enhance the integrity, efficiency, orderliness, and competitiveness of the nation's financial markets and their ability to maintain investor confidence. A significant part of this mission is related to cybersecurity and other operational risks.

The Board is also a member of the FBIIC, which is chartered under the PWGFM. The FBIIC consists of federal and state financial regulatory agencies that supervise banking, investment, and insurance firms, and is chaired by the U.S. Department of the Treasury (Treasury). FBIIC members engage in efforts to strengthen the security and resilience of critical infrastructure across the financial services sector including financial institutions regulated and supervised by the FBIIC member organizations. Additionally, the Federal Reserve participated with other FBIIC members providing enhancements to the FBIIC All-Hazards Incident Response Plan that augments coordination among the agencies when responding to a cyber incident impacting the financial sector.

The Board, along with other regulatory agencies, financial institutions, and trade associations, participates in the FBIIC's periodic cybersecurity exercises. These exercises have proved useful in advancing incident management and information-sharing protocols across the financial services

sector. Additionally, through participation in these exercises, the Board has improved its ability to respond to, in coordination with other financial regulators, potential operational disruptions in the financial services sector's critical infrastructure. These exercises also have led to the creation of private sector-led and public sector-supported initiatives to enhance cybersecurity resilience. These include capabilities to proactively identify, analyze, and coordinate activities to mitigate systemic risk to the U.S. financial system (and other critical infrastructure) from cybersecurity threats.

In addition, as a member of the FFIEC, which is an interagency body that promotes uniformity and consistency in the examination of financial institutions across its members, the Board actively coordinates with other FFIEC members on cybersecurity risk management issues. The Board contributes to the efforts of the FFIEC in responding to cybersecurity incidents affecting institutions supervised by FFIEC members. In addition, the Board also supports ongoing dialogue on cybersecurity issues and opportunities to improve consistency in examination approaches.

The Cybersecurity and Critical Infrastructure Subcommittee (CCIS) continued to work on key cybersecurity areas, including risk management and oversight, threat intelligence and collaboration, cybersecurity controls, and cybersecurity incident management and resilience. This includes a continued focus on the development of cybersecurity resources for supervised institutions, including materials to assist banks with cybersecurity assessment following the sunset of the FFIEC Cybersecurity Assessment Tool on August 31, 2025. The FFIEC IT Subcommittee continued to maintain and update the FFIEC IT Handbook and its component booklets.²² In August 2025, the subcommittee sponsored its annual IT conference for examiners that highlighted current and emerging technology issues affecting supervised institutions.

The Board also continued to contribute to and monitor the Cybersecurity and Infrastructure Security Agency's (CISA) development of cross-sector cybersecurity performance goals (CPGs), voluntary practices that businesses and critical infrastructure owners can take to protect themselves against cybersecurity threats. CISA released updated CPGs in December 2025.²³ The Board is reviewing these CPGs for any necessary action.

Public and Private Sector Coordination

The Board participates in various public-private partnerships to enhance cybersecurity resilience in the financial system. Through FBIIC, the Board coordinates with the Financial Services Sector Coordinating Council (FSSCC), a nonprofit body composed of more than 70 members from across the financial services industry whose mission is to strengthen the resiliency of the financial services sector. This partnership focuses on improving the financial services sector's ability to rapidly

²² See FFIEC website for IT Booklets, <https://ithandbook.ffiec.gov/it-booklets/>.

²³ See "Cross-Sector Cybersecurity Performance Goals," Cybersecurity and Infrastructure Security Agency, <https://www.cisa.gov/cross-sector-cybersecurity-performance-goals>.

respond to and recover from significant cybersecurity incidents, thereby reducing the potential for such incidents to threaten the stability of the financial system and the broader economy. In the past several years, the FBIIC has engaged with the FSSCC in several areas relating to cybersecurity, cloud adoption, AI, data protection, and incident response. Most recently, the Federal Reserve and other FBIIC members participated in discussions to inform the development of joint Treasury–FSSCC products related to cybersecurity considerations for AI.²⁴ Additionally, Board staff worked with regulatory partners within the FBIIC to address industry questions regarding the protection of supervisory data by federal financial regulators that were raised through the FBIIC-FSSCC partnership.

The Board also participated in industry-led initiatives to enhance cybersecurity risk management. For example, the Board is a member of the Financial Services Information Sharing and Analysis Center (FS-ISAC), the global financial industry’s resource for cybersecurity- and physical-threat intelligence analysis and sharing. The Board encourages its supervised institutions to incorporate threat monitoring programs and participate in information sharing organizations such as the FS-ISAC. Outside of FS-ISAC, the Board also participates in other information sharing and analysis organizations, which include trade associations, third-party threat intelligence services, and specialized information-sharing arrangements. The Board encourages voluntary cybersecurity information sharing through CISA, which provides platforms for sharing situational awareness and response efforts, as appropriate, to current cybersecurity, communications, and physical incidents.

Over the past few years, Board staff have conducted more focused outreach to community banking organizations on cybersecurity matters outside of ongoing supervision. The goal of this ongoing work is to elevate resilience by enhancing community bankers’ understanding of the cybersecurity-risk environment, increasing awareness of existing guidance and tools, and sharing effective practices available to help mitigate cybersecurity risks. This outreach is intended to strengthen and improve coordination before, during, and following cybersecurity incidents, and Board staff have produced a series of webinars, articles, presentations, and resources for community banks.

The Board also participated in the planning and execution of public-private “Hamilton Series,” cybersecurity exercises lead by the Treasury with other U.S. government agencies, the FSSCC, and FS-ISAC, to develop cybersecurity exercises aimed at improving responses to a range of cybersecurity-threat scenarios within the U.S. financial sector. In 2025, the Board, along with the Treasury, facilitated additional in-person tabletop exercises with participants from smaller banking

²⁴ See U.S. Department of the Treasury, “Treasury Releases Two New Resources to Guide AI Use in the Financial Sector,” press release, February 19, 2026, <https://home.treasury.gov/news/press-releases/sb0401>.

organizations as part of the Hamilton Series. These cyber exercises help prepare the financial and public sectors to respond to cyberattacks and operational disruptions.

For several years, the Federal Reserve has partnered with industry and the Treasury to increase our collective focus on payments' resilience. With sponsorship from the Treasury, the Analysis and Resilience Center for Systemic Risk (ARC) launched the Systemic Payments Infrastructure Initiative in 2023. Federal Reserve Financial Services (FRFS), on behalf of the 12 Federal Reserve Banks, became a member of the ARC and an active participant in the Systemic Payments Infrastructure Initiative. Through this initiative, the ARC and FRFS continued to assess opportunities to improve wholesale payments resilience.

International Coordination

The Board participates in cybersecurity activities undertaken by groups such as the Financial Stability Board (FSB), the Basel Committee on Banking Supervision (BCBS), the Committee on Payment and Market Infrastructures (CPMI) (and its joint efforts with the International Organization of Securities Commissions (IOSCO)), the International Association of Insurance Supervisors (IAIS), and the Group of Seven (G-7).

The BCBS acts as the primary forum for international coordination on the prudential regulation of banks and cooperation on banking supervisory matters. In March 2021, the BCBS issued the Principles for Operational Resilience²⁵ and the Principles for the Sound Management of Operational Risk.²⁶ These documents highlight the importance of sound operational risk management, including cybersecurity risk management, and are aligned with guidance released by the Board on operational resilience.²⁷ In September 2021, the BCBS published a newsletter calling for increased efforts to improve banks' resilience to cybersecurity threats, intended to complement earlier actions and promote widespread adoption of measures to strengthen banks' cybersecurity.²⁸ The BCBS issued the Consultative Document in July 2023 to update the 2005 Joint Forum Paper on Outsourcing, which is related to third-party risk. In December 2025, the BCBS published the updated version of that document which identified and described 12 principles for sound management of third-party risk, including governance, risk management, strategy, risk assessments, and due diligence.²⁹

²⁵ See Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Bank for International Settlements, March 2021), <https://www.bis.org/bcbs/publ/d516.pdf>.

²⁶ See Basel Committee on Banking Supervision, *Revisions to the Principles for the Sound Management of Operational Risk* (Bank for International Settlements, March 2021), <https://www.bis.org/bcbs/publ/d515.pdf>.

²⁷ See Board of Governors of the Federal Reserve System, "Interagency Paper on Sound Practices to Strengthen Operational Resilience," SR letter 20-24 (November 2, 2020), <https://www.federalreserve.gov/supervisionreg/srletters/SR2024.htm>.

²⁸ See Bank for International Settlements, "Basel Committee Calls for Improved Cyber Resilience, Reviews Climate-Related Financial Risks and Discusses Impact of Digitalization," press release, September 20, 2021, <https://www.bis.org/press/p210920a.htm>.

²⁹ See Basel Committee on Banking Supervision, *Principles for the sound management of third-party risk* (Bank for International Settlements, December 2025), <https://www.bis.org/bcbs/publ/d605.pdf>.

Through the FSB, the Board participated in the development and release of the Format for Incident Reporting Exchange (FIRE) in April 2025. FIRE is a common framework developed collaboratively with financial authorities and industry that financial firms can use to report cyber and other operational incidents. It is an optional and flexible resource that was designed to promote consistency and enhance communication among financial authorities and industry.³⁰ Further, the FSB recently published a consultative paper on the use of AI in financial services, which includes a section on sound practices for cybersecurity and AI.³¹

Through the CPMI-IOSCO, the Board has played a key role in the development of the Principles for Financial Market Infrastructures (PFMI) and related guidance for FMIs, including the Cybersecurity Resilience Guidance. The CPMI-IOSCO continues to monitor and analyze emerging risks that could affect the safety and efficiency of FMIs, including cybersecurity and third-party risks. The Board contributes to the development of IAIS's annual key financial stability priorities for insurance providers, which was most recently released in January 2024.³² Among the priorities is a focus on growing cybersecurity risks, which continues to create significant impacts to insurers' financial liabilities. In 2023, the Board contributed to the IAIS's *Global Insurance Market Report*.³³ This analysis focuses on risks and trends associated with cybersecurity insurance coverage, cybersecurity resilience in the insurance sector, and the impact these risks may have on financial stability.

Given the rapidly evolving nature of cybersecurity risks and the cross-border and cross-sector relevance of cybersecurity threats, the Federal Reserve continued to participate in the G-7 Cyber Expert Group (CEG), a working group established by the G-7 finance ministers, central bank governors, and other financial authorities to elevate cybersecurity concerns and enhance cooperation among G-7 jurisdictions and the financial services sector. The Federal Reserve has contributed to current G-7 cybersecurity priorities, including coordinated cyber incident response, cyber incident exercises, identification of current and emerging cyber risks, and development of resources related to the cybersecurity implications of emerging technologies.

³⁰ See Financial Stability Board, "Format for Incident Reporting Exchange (FIRE): Final Report," April 15, 2025, <https://www.fsb.org/2025/04/format-for-incident-reporting-exchange-fire-final-report/>.

³¹ See Financial Stability Board, "FSB Consults on Sound Practices for the Responsible Adoption of Artificial Intelligence," June 10, 2026, <https://www.fsb.org/2026/06/fsb-consults-on-sound-practices-for-the-responsible-adoption-of-artificial-intelligence-ai/>.

³² See International Association of Insurance Supervisors, "IAIS sets strategic direction for 2025–2029," press release, October 22, 2024, <https://www.iais.org/2024/10/iais-sets-strategic-direction-for-2025-2029/>.

³³ See International Association of Insurance Supervisors, *Global Insurance Market Report (GIMAR)*, Special Topic Edition on Cyber, (International Association of Insurance Supervisors, April 2023) <https://www.iaisweb.org/uploads/2023/04/GIMAR-2023-special-topic-edition-on-cyber.pdf>.

In September 2025, the G-7 CEG published papers on cybersecurity considerations for AI³⁴ and fundamental elements of collective cybersecurity incident response and recovery in the financial sector.³⁵ In June 2025, the G-7 CEG published a paper on reconnection following cyber incidents.³⁶ In September 2024, the G-7 CEG released a statement titled “Planning for the Opportunities and Risks of Quantum Computing,” which reflects growing concerns among international financial regulatory authorities that cybersecurity threat actors will eventually be able to use quantum computers to defeat banks’ current cryptographic techniques that secure communications and IT systems. The G-7 CEG encourages jurisdictions to monitor developments in quantum computing, to promote collaboration among relevant public and private stakeholders, and to begin planning for the potential risks posed by quantum computing on some current encryption methods.³⁷ This work was continued with the release of the G-7 CEG’s statement on a coordinated roadmap for the transition to post-quantum cryptography in the financial sector, released in January 2026.³⁸

Board Internal

The Board places a strong emphasis on promoting cybersecurity risk management through active collaboration and coordination across agency stakeholders. To achieve this goal, the Board’s Office of the Chief Operating Officer (OCOO) facilitates timely exchange of information regarding cybersecurity risk issues across divisions, including business, IT, and information security functions. This approach ensures that cross-functional perspectives are taken into account, enabling the Board to coordinate its efforts and develop cohesive cybersecurity policy. Board security personnel take an active role in other coordination activities, collaborating with groups within the System, as well as participating in interagency cybersecurity forums and working groups facilitated by CISA. This collaboration helps Board staff better identify and respond to potential threats. The Board is an active participant in CISA’s Continuous Diagnostics and Mitigation program, which is a governmentwide effort to improve cybersecurity risk management across all federal agencies. The Continuous Diagnostics and Mitigation program provides tools and services to help agencies identify and prioritize cybersecurity risks, improve visibility into their networks, and make informed decisions about how to address those risks.

³⁴ See U.S. Department of the Treasury, “G-7 Cyber Expert Group Statement on Artificial Intelligence and Cybersecurity,” press release, September 2025, <https://home.treasury.gov/system/files/136/G7-Cyber-Expert-Group-Statement-AI-and-Cybersecurity-2025.pdf>.

³⁵ See U.S. Department of the Treasury, “G-7 Fundamental Elements of Collective Cyber Incident Response and Recovery in the Financial Sector,” <https://home.treasury.gov/system/files/136/G7-CEG-Fundamental-Elements-CCIRR-2025.pdf>.

³⁶ See U.S. Department of the Treasury, “G-7 Cyber Expert Group: Reconnection Framework Best Practice,” <https://home.treasury.gov/system/files/216/G7-CEG-Reconnection-Framework-Best-Practice.pdf>.

³⁷ See U.S. Department of the Treasury, “G-7 Cyber Expert Group Statement on Planning for the Opportunities and Risks of Quantum Computing,” press release, September 2024, <https://home.treasury.gov/system/files/136/G7-CYBER-EXPERT-GROUP-STATEMENT-PLANNING-OPPORTUNITIES-RISKS-QUANTUM-COMPUTING.pdf>.

³⁸ See U.S. Department of the Treasury, “G-7 Cyber Expert Group Statement on Advancing a Coordinated Roadmap for the Transition to Post-Quantum Cryptography in the Financial Sector,” press release, January 2026, <https://home.treasury.gov/system/files/136/G7-CEG-Quantum-Roadmap.pdf>.

Board OIG Assessment of the Board's Progress in Implementing Key FISMA Information Security Program Requirements

To support the annual independent evaluation of agency information security programs by inspectors general (IGs) under the Federal Information Security Modernization Act (FISMA), the Department of Homeland Security publishes FISMA reporting metrics. These metrics direct IGs to evaluate the effectiveness of agency information security programs across various attributes that are grouped into security domains.³⁹ In 2025, a new governance domain was introduced as part of the OIG's annual FISMA maturity assessment of the Board's information security program in alignment with the six security functions as defined by the NIST Cybersecurity Framework (CSF) 2.0. The six security functions defined by NIST CSF 2.0 are as follows: *govern, identify, protect, detect, respond, and recover*.⁴⁰

Pursuant to the FISMA reporting metrics, IGs assess the effectiveness of each of the six NIST CSF 2.0 functions using a maturity model spectrum. The five levels of the IG FISMA maturity model are ad hoc (level 1), defined (level 2), consistently implemented (level 3), managed and measurable (level 4), and optimized (level 5). Within the context of the maturity model, a level 4 information security program is considered to be operating at an effective level of security. The OIG's 2025 assessment of the Board's overall information security program rated the program as "not effective" or a level 3 maturity.⁴¹

Prior to the 2025 audit, the Board had already identified weaknesses within the governance domain that had the potential to impact the program's overall effectiveness. The Board has begun executing a new information security operating model to address those weaknesses. The identified weaknesses are primarily a result of governance challenges, as confirmed by multiple third-party security assessments of the Board's security posture. After this audit was completed, the IG was made aware of the technical security assessments and acknowledged the conclusion that all weaknesses were primarily non-technical and limited to the governance domain. The Board's maturity scores in the other domains have either increased or remained stable.

The Board continues to focus on improving the aspects of the information security program that require correction to return to a level 4 maturity and recover the Board's effective rating. With additional effort in governance, the gap is expected to be closed in the coming audits. The Board's

³⁹ See "FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0," Cybersecurity and Infrastructure Security Agency, last modified on April 3, 2025, https://www.cisa.gov/sites/default/files/2025-04/Final%20FY%202025%20IG%20FISMA%20Reporting%20Metrics_Ver%202.0_April%202025-508_0.pdf.

⁴⁰ See "NIST Cybersecurity Framework (CSF) 2.0," National Institute of Standards and Technology, February 26, 2024, <https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf>. The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

⁴¹ See Board of Governors of the Federal Reserve System, Office of Inspector General, *2025 Audit of the Board's Information Security Program* (Board of Governors, October 2025), <https://oig.federalreserve.gov/reports/board-information-security-program-redacted-oct2025.pdf>.

efforts also include continued prioritization of the protection of its operations and assets through ongoing assessments and improvements of its security posture.

The Board's Ongoing Efforts to Strengthen Its Information Security Program

The Board also places strong emphasis on maintaining a comprehensive security and privacy control program, which is supported by a centralized Plan of Action and Milestones (POA&M) process. This process ensures that plans are developed in response to any finding or weakness identified in security and privacy control implementations. In addition, the POA&M process is used to track and report on the remediation of findings and status of recommendations issued by the OIG, as well as weaknesses identified through internal controls testing. Board staff are committed to making progress on closing outstanding POA&Ms.

The Board continues to improve its cybersecurity posture and protect against cybersecurity threats. Efforts include investing in technical controls such as firewalls, intrusion detection and prevention systems, and security information and event management systems to monitor and detect potential threats. The Board follows FISMA and related NIST standards and guidance and implements the necessary controls to protect our information systems. In addition, the Board engages third-party security experts to perform regular assessments and testing to identify opportunities to improve its security posture. Finally, the Board has implemented a layered security architecture, which includes multiple layers of defense such as network segmentation, access controls, and encryption to better protect non-public information.

The Board also continues to enhance its information security architecture. One of the Board's top priorities is the continued implementation of a zero-trust security model, which will provide an additional layer of security to protect its systems and data, as well as implementing web application security measures to identify and address vulnerabilities in the Board's web applications. The Board is also continuing to enhance its existing supply chain risk-management policies and procedures to account for necessary security requirements for cloud systems and capabilities, such as updates to the Board's incident response and data protection policies.

Current or Emerging Threats to Financial System Resilience

The Board actively monitors cybersecurity risks and emerging threats through internal Federal Reserve programs and resources, the supervisory process, and coordination with financial regulatory agencies and other government agencies, as well as the private sector. Given the highly interconnected nature of the financial sector and its dependencies on critical service providers, all participants in the financial system face cybersecurity threats.

Various threat actors, including ones that are financially motivated, ideologically driven, and foreign government-controlled, have all conducted cyberattacks and intrusions against the U.S. financial sector. Increased internet-based interconnectedness between financial institutions and dependence on third-party service providers can result in cybersecurity incidents impacting multiple organizations and can have potentially systemic consequences. Such incidents could affect the ability of targeted firms to provide services and conduct business as usual, presenting a unique challenge to operational resilience. These incidents can also threaten the confidentiality, integrity, and availability of the targeted firm's data.

Given the evolving cybersecurity-threat landscape, domestic financial institutions have maintained a heightened state of preparedness. The Board, Office of the Comptroller of the Currency, and Federal Deposit Insurance Corporation are closely monitoring developments related to these types of threats and have not observed material impacts on the financial sector.

Artificial Intelligence

In the last year, a new set of frontier AI models emerged with unique implications for cybersecurity. Leading researchers report that these new models can identify previously undiscovered vulnerabilities, create methods to exploit them, and link multiple vulnerabilities in a “chain of exploits” that can be executed to attack a target at machine speeds. Due to the apparent power of these models, mainstream AI firms are rolling out their availability on a controlled basis. This presents an opportunity to identify and address vulnerabilities before attackers can exploit them. However, the introduction of such models raises the risk that malicious actors could gain access to vulnerability information or offensive AI capabilities before the vulnerabilities are fully addressed across the financial sector and the cyber ecosystem at large.

In light of these risks, there is a need to promote the responsible use of AI, to use the current tools at our disposal to identify and address vulnerabilities, and to share information appropriately for the benefit of the financial sector.

The Board remains aligned with the U.S. government and the financial sector writ large in its approach to AI adoption and risk management. The Board will continue to partner with the financial sector and other federal regulators, federal banking agencies, and financial institutions to secure financial infrastructure and manage risk.

Geopolitical Tensions

The financial sector is potentially vulnerable to foreign conflicts and the activities of nation-state actors, both directly and indirectly, because of the interconnectedness of global financial markets and reliance on international digital networks.⁴² Adverse geopolitical events increase the likelihood of cyberattacks with the intent of disrupting critical infrastructure, including financial services, or undermining trust in public and private-sector institutions. Destructive malware tools and methods used to destroy or corrupt critical data have been employed and observed.⁴³ These methods are evolving in sophistication and capability. Geopolitical tensions may create motivations and opportunities for malicious actors aiming to employ cyberattacks to advance or harm the interest of participants in these conflicts, such as by targeting financial infrastructure.

Cyber-Criminal Activity

The global cyber-criminal ecosystem continues to remain a top threat to the U.S. financial sector. Cyberattacks may disproportionately affect small community and regional banking organizations that do not have sufficient resources and capabilities to defend against sophisticated actors.

Cyber-criminal methods and resource offerings that pose a risk to financial institutions' ability to operate and protect customer data may include:

- **Ransomware as a Service (RaaS).** The RaaS ecosystem, where threat actors create “franchised” variants of ransomware, remains dynamic with groups disbanding and sometimes rebranding under different names. Despite activity from law enforcement aimed at disrupting ransomware operations, attacks associated with RaaS increased year-over-year from 2023 to 2024 across sectors and geographies and increased year over-year within the financial sector.⁴⁴

⁴² See U.S. Department of the Treasury, *2022 Annual Report: Financial Stability Oversight Council* (Department of the Treasury, 2022), <https://home.treasury.gov/system/files/261/FSOC2022AnnualReport.pdf>.

⁴³ See Cybersecurity and Infrastructure Security Agency, “U.S. and International Partners Release Report on Russian Cyber Actors Using ‘Infamous Chisel’ Malware,” press release, August 31, 2023, <https://www.cisa.gov/news-events/news/us-and-international-partners-release-report-russian-cyber-actors-using-infamous-chisel-malware>.

⁴⁴ See U.S. Department of Justice, “U.S. Department of Justice Disrupts Hive Ransomware Variant,” press release, January 26, 2023, <https://www.justice.gov/opa/pr/us-department-justice-disrupts-hive-ransomware-variant>.

- **Phishing.** Threat actors continue to evolve their techniques for targeting email to establish initial access for future malicious activity and exfiltrate sensitive information. The ongoing use of AI to develop highly sophisticated phishing campaigns and deep fakes continues to impact the financial sector.⁴⁵ Attackers target email to deliver malware, gain access to organizational credentials, and other social engineering techniques. Examples of improved techniques include subverting security controls on endpoints, embedding quick-response (QR) codes within malicious messages, and intercepting one-time passwords from users.
- **Increasing commoditization of tools associated with cyber crime.** In addition to RaaS, financially motivated threat actors are creating various “services” that are used within attacks against organizations that are part of or support the financial sector. Examples of these “services” include malware-as-a-service (MaaS) and phishing-as-a-service (PhaaS). Threat actors can leverage these “services” for a nominal amount of money, effectively enabling lower-tier attackers to conduct moderately sophisticated campaigns. Threat actors are also continuing to work together to increase the effectiveness of attacks. Examples of this cooperation include selling information among themselves or selling initial access into victim organizations.
- **Exploitation of vulnerabilities.** Malicious actors have impacted financial sector organizations through exploiting both “zero-day” (patches not available) and “n-day” (patches available but not yet applied) vulnerabilities.⁴⁶ The sharing of technical information by threat actors and their efforts to reverse engineer patches often shortens the window between patch application and observed exploitation activity. As evidenced by the increasing number of published vulnerabilities year-over-year, organizations should regularly review and update IT systems and controls for security against evolving threats. This exploitation activity also emphasizes the importance of a defense-in-depth security posture where a breakdown in one control does not lead to widespread compromise.
- **Distributed denial-of-service attacks.** Despite the evolution in techniques and increasing peak volume, the major anti-distributed denial of service (DDoS) services remain relatively well-positioned to defend against these attacks. DDoS attacks continue to evolve and threat actors can also leverage an increasing number of DDoS services that are available for sale on dark web forums and marketplaces.

Cybersecurity Risks Associated with Third-Party Providers

Financial institutions rely heavily on third-party service providers for critical business functions and a cyberattack against a third party, vendor, or technology partner can have a significant impact. In

⁴⁵ See Michael S. Barr, “Deepfakes and the AI Arms Race in Bank Cybersecurity,” speech delivered at the Federal Reserve Bank of New York, New York, NY, April 17, 2025, <https://www.federalreserve.gov/newsevents/speech/barr20250417a.htm>.

⁴⁶ See Cybersecurity and Infrastructure Security Agency, “#StopRansomware: LockBit 3.0 Ransomware Affiliates Exploit CVE 2023-4966 Citrix Bleed Vulnerability,” press release, November 21, 2023, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa23-325a>.

recent years, this interdependency risk has been highlighted by the attacks against trading platforms and multiple providers within the mortgage-servicing ecosystem.⁴⁷ This risk was highlighted again in 2025 by the ongoing attacks against vendor-provided network devices and services.⁴⁸

Financial institutions have also moved portions of their IT infrastructure to cloud-computing platforms to increase computing capacity, flexibility, and lower costs. Despite the many benefits of cloud service providers, there are also risks associated with adopting cloud services that are different from the risks associated with traditional data center environments. In the last few years, there have been several reports addressing the risks associated with using cloud services, including the Treasury's 2023 report outlining trends, risks, and challenges related to the adoption of cloud services by the financial services sector;⁴⁹ the National Security Agency's (NSA) cloud best practices report;⁵⁰ and CISA's information sheet that also addressed best practices for cloud security.⁵¹ These reports encourage upholding the cloud shared responsibility model, using secure cloud identity and access management practices, implementing network segmentation and encryption in cloud environments, and mitigating risks from managed service providers in cloud environments.

Third-party service providers, including fintech firms, can offer consumers access to new or better services, but such arrangements may provide malicious actors with additional avenues to gain access to private data. For example, improperly configured application programming interfaces, which provide gateways into financial institutions' information (often relied on by fintech platforms for information sharing), may increase the risk of data breaches, especially of customers' personal or sensitive information.

The Federal Reserve continues to engage with the Treasury and other federal (and state) agencies and the private sector to address risks associated with third-party dependencies.

⁴⁷ See Harry Robertson, "ION brings clients back online after ransomware attack – source," *Reuters*, February 7, 2023, <https://www.reuters.com/technology/ion-starts-bring-clients-back-online-after-ransomware-attack-source-2023-02-07/>; Laura Matthews, "EquiLend hack raised costs as traders flew blind, sources say," *Reuters*, February 26, 2024, <https://www.reuters.com/technology/cybersecurity/equilend-hack-raised-costs-traders-flew-blind-sources-say-2024-02-26/>; and "Recent Cyberattacks Impact Financial Services Sector," State of New Jersey, February 22, 2024, <https://www.cyber.nj.gov/Home/Components/News/News/1192/214>.

⁴⁸ See Cybersecurity and Infrastructure Security Agency, "2025 Year in Review," <https://www.cisa.gov/about/2025YIR>.

⁴⁹ See U.S. Department of the Treasury, "The Financial Services Sector's Adoption of Cloud Services," <https://home.treasury.gov/system/files/136/Treasury-Cloud-Report.pdf>.

⁵⁰ See National Security Agency, "NSA Releases Top Ten Cloud Security Mitigation Strategies," press release, March 7, 2024, <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3699169/nsa-releases-top-ten-cloud-security-mitigation-strategies/>.

⁵¹ See Cybersecurity and Infrastructure Security Agency, "CISA and NSA Release Cybersecurity Information Sheets on Cloud Security Best Practices," press release, March 7, 2024, <https://www.cisa.gov/news-events/alerts/2024/03/07/cisa-and-nsa-release-cybersecurity-information-sheets-cloud-security-best-practices>.

Emerging Quantum-Related Risks

Quantum computing is another significant emerging risk area on the horizon, as quantum computing capabilities could render some of the encryption standards that are most widely used by financial institutions obsolete. The introduction of post-quantum cryptography, or encryption algorithms that remain viable once quantum computing is available, will provide new solutions for protecting the integrity and confidentiality of data. Several federal agencies have highlighted steps that institutions can take now to prepare for the cryptographic risks associated with quantum computing. For example, in 2023, the Cybersecurity and Infrastructure Security Agency, National Security Agency, and National Institute of Standards and Technology published “Quantum-Readiness: Migration to Post-Quantum Cryptography,” which informs institutions about quantum capabilities and promotes a proactive approach for institutions to take now by instituting a “Quantum-Readiness Roadmap” to prepare for post-quantum cryptography migration.⁵² The National Institute of Standards and Technology finalized its initial set of quantum-resistant encryption algorithms in August 2024.⁵³ As discussed previously, the Federal Reserve has participated with the G-7 Cyber Expert Group on the release of two informational publications related to the migration to post-quantum cryptography in the financial sector.

Risks such as these highlight the importance of collective actions across the government and strong collaboration with the private sector in advancing measures to understand and mitigate risks. Cybersecurity risk mitigation and cybersecurity resilience initiatives continue to be high priorities for the Federal Reserve. Through policymaking, supervision of financial institutions and other entities overseen or operated by the Federal Reserve, and internal policies aimed at mitigating cybersecurity threats, the Federal Reserve continues to maintain a strong internal resilience posture and promote resilience across the U.S. financial sector.

⁵² See National Security Agency, “Quantum-Readiness: Migration to Post-Quantum Cryptography,” press release, August 21, 2023, <https://www.nsa.gov/Press-Room/Press-Releases-Statements/Press-Release-View/Article/3498776/post-quantum-cryptography-cisa-nist-and-nsa-recommend-how-to-prepare-now/>.

⁵³ See National Institute of Standards and Technology, “NIST Releases First 3 Finalized Post-Quantum Encryption Standards,” press release, August 13, 2024, <https://www.nist.gov/news-events/news/2024/08/nist-releases-first-3-finalized-post-quantum-encryption-standards>.

Find other Federal Reserve Board publications at www.federalreserve.gov/publications/default.htm,
or visit our website to learn more about the Board and how to connect with us on social media.



www.federalreserve.gov

0926