REPORT TO CONGRESS

Cybersecurity and Financial System Resilience Report

July 2022

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

The Federal Reserve System 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.

REPORT TO CONGRESS

Cybersecurity and Financial System Resilience Report

July 2022

BOARD OF GOVERNORS OF THE FEDERAL RESERVE SYSTEM

Contents

Overview

The Consolidated Appropriations Act, 2021[1] (CAA) requires the Federal Reserve Board (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 and emerging cyber 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 and Board-supervised institutions. The Board and the Reserve Banks maintain robust information security programs and engage and coordinate on cybersecurity issues with numerous critical stakeholders including the federal banking agencies, other government 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 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 programs. As part of its safety and soundness supervision, the Board issues cybersecurity-related regulations and guidance, examines and monitors supervised institutions' cybersecurity risk-management posture, and collects data on cyber incidents (along with the other federal financial regulatory agencies) to monitor trends in the financial services sector. Additionally, the Board and the Reserve Banks secure their internal information and information assets 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 and guidance for supervised institutions regarding IT risk management, cybersecurity, operational resilience, and other related topics.[2]

The Board and other regulatory agencies also publish interagency guidance on various aspects of information security risk within the financial services sector. For example, the Interagency Guidelines Establishing Information Security Standards impose requirements on banking organizations to develop and implement administrative, technical, and physical safeguards to promote the security, confidentiality, and integrity of customer information.[3]

In addition, the Board utilizes general safety and soundness guidelines to mitigate cyber risk.[4]

---

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

[4] See Interagency Guidelines Establishing Standards for Safety and Soundness Standards, 12 C.F.R. pt. 30, appendix A (proposed July 10, 1995).

These guidelines require banks to have internal controls and information systems appropriate to the size of the institution and to the nature, scope, and risk of its activities and that provide for, among other requirements, effective risk assessment and adequate procedures to safeguard and manage assets. The safety and soundness standards also require banks to have internal audit systems that provide for adequate testing and review of information systems. See table 1 for recent Board actions and actions in collaboration with other financial regulatory agencies to promote cybersecurity.

Further, the Board's domestic regulatory, supervisory, and oversight framework for financial market infrastructures (FMIs) consists of the Board's Regulation HH and part I of the Federal Reserve Policy on Payment System Risk (PSR policy). Regulation HH imposes risk-management standards on "financial market utilities" (FMUs)[5] that the Financial Stability Oversight Council has designated as systemically important under title VIII of the Dodd-Frank Act (title VIII).[6] Part I of the PSR policy sets out risk-management standards for certain FMIs that are not subject to Regulation HH, including payment and settlement systems operated by the Reserve Banks. The risk-management standards in Regulation HH and the PSR Policy reflect the relevant international standards for these FMIs—the *Principles for Financial Market Infrastructures*, or PFMI issued by the Committee on Payments and Market Infrastructures and the International Organization of Security Commissions (CPMI-IOSCO).[7] Several of these standards are relevant to the management and mitigation of cyber risk, including standards related to governance, operational risk (including cybersecurity risks), and comprehensive risk management.

The Board's FMI supervisory teams also utilize other relevant cybersecurity risk guidance, such as the CPMI-IOSCO's *Guidance on Cyber Resilience for Financial Market Infrastructures* (Cyber Resilience Guidance),[8] to supplement the PFMI operational risk-management expectations. Additionally, following a rise in incidents where threat actors exposed weak cybersecurity practices at firms that participate in FMIs, the CPMI published a strategy on reducing the risk of wholesale payments fraud related to endpoint security.[9]

---

[5] The term *FMU* is defined under title VIII and generally refers to payment, clearing, and settlement systems. The term *FMI* is used internationally. FMUs are a subset of FMIs—in particular, the term FMI includes trade repositories while the term FMU does not.

[6] See 12 C.F.R. pt. 234. The risk-management standards in Regulation HH apply to designated FMUs for which the Board is the lead supervisory agency, while comparable CFTC and SEC regulations apply to other designated FMUs.

[7] See Committee on Payment and Settlement Systems and Technical Committee of the International Organization of Securities Commissions, *Principles for Financial Market Infrastructures* (Basel: Bank for International Settlements, April 2012), https://www.bis.org/cpmi/publ/d101a.pdf. *Principles for Financial Market Infrastructures* and subsequent supplemental guidance documents were issued by the international standard-setting bodies for FMIs: the Committee on Payments and Market Infrastructures of the Bank for International Settlements and the International Organization of Securities Commissions (CPMI-IOSCO).

[8] See Committee on Payments and Market Infrastructures and the Board of the International Organization of Securities Commissions (IOSCO), *Guidance on Cyber Resilience for Financial Market Infrastructures* (Basel: Bank for International Settlements, June 2016), https://www.bis.org/cpmi/publ/d146.htm.

[9] See Committee on Payments and Market Infrastructures, *Reducing the Risk of Wholesale Payments Fraud Related to Endpoint Security* (Basel: Bank for International Settlements, May 2018), https://www.bis.org/cpmi/publ/d178.htm.

Table 1. Recent Board and interagency actions to promote cybersecurity

Date	Action
June 30, 2021	The Board published Supervision and Regulation letter (SR letter) 21-11 notifying supervised institutions that the Federal Financial Institutions Examination Council (FFIEC) issued the "FFIEC Architecture, Infrastructure, and Operations Examination Handbook," one of the 11 booklets that compose the FFIEC Information Technology Examination Handbook (IT Handbook). The booklet provides guidance to examiners when assessing the risk profile and adequacy of an entity's information technology architecture, infrastructure, and operations.[1]
July 19, 2021	The Board, Federal Deposit Insurance Corporation (FDIC), and the Office of the Comptroller of the Currency (OCC) proposed and requested comment on third-party risk-management guidance designed to help banking organizations manage risks associated with third-party relationships, including relationships with financial technology-focused entities. Insufficient management of third-party risks could lead to systemic vulnerabilities. A cyber incident or an operational outage at a third party, such as an IT service provider, may result in spillover effects or may have significant systemic implications in the financial services sector. Banking organizations that engage third parties to provide products or services or to perform other activities remain responsible for ensuring that such outsourced activities are conducted in a safe and sound manner and in compliance with all applicable laws and regulations, including consumer protection laws. The proposed guidance is intended to assist banking organizations in identifying and addressing the risks associated with third-party relationships and respond to industry feedback requesting consistency among the agencies with respect to third-party risk-management guidance. The extended comment period for the proposed guidance closed on October 18, 2021, and the agencies are reviewing the comments received
August 11, 2021	The Board and other FFIEC agencies issued the interagency guidance titled "Authentication and Access to Financial Institution Services and Systems" to provide financial institutions with examples of effective risk-management principles and practices for access and authentication.[2] The principles and practices address customers, employees, and third parties that access digital banking services and financial institution information systems. The guidance highlights risk-management practices that support oversight of identification, authentication, and access solutions as part of an institution's information security program. The guidance acknowledges significant risks associated with the cybersecurity threat landscape that reinforce the need for financial institutions to effectively authenticate users and customers to protect information systems, accounts, and data
August 27, 2021	The Board, FDIC, and OCC issued a guide entitled "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks."[3] The guide is a resource for community banks when performing due diligence on prospective relationships with fintech companies. While the guide is written from a community bank perspective, the fundamental concepts may be useful for banks of varying size and for other types of third-party relationships. The guide aligns with existing regulations and guidance that address due diligence and third-party risk management and is consistent with the risk-management principles in the July 19, 2021, proposed interagency guidance.
November 18, 2021	Federal bank regulatory agencies promulgated a final rule to improve the sharing of information about cyber incidents that may affect the U.S. banking system. [4] The final 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 cyber incident has occurred. Notification is required 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. In addition, the final rule requires a bank service provider to notify 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 banking organization customers for four or more hours. Compliance with the final rule is required as of May 1, 2022.

[1] See SR letter 21-11, "FFIEC Architecture, Infrastructure, and Operations Examination Handbook," https://www.federalreserve.gov/supervisionreg/srletters/SR2111.htm. The guidance applies to all institutions supervised by the Federal Reserve, including those with $10 billion or less in consolidated assets. The FFIEC was established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978, Public Law 95-630. The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms and to make recommendations to promote uniformity in the supervision of financial institutions supervised by the Board, the FDIC, the National Credit Union Administration, the OCC, and the Consumer Financial Protection Bureau.

[2] See SR letter 21-14, "Authentication and Access to Financial Institution Services and Systems," https://www.federalreserve.gov/supervisionreg/srletters/sr2114.htm.

[3] See SR letter 21-15, "Conducting Due Diligence on Financial Technology Companies: A Guide for Community Banks," https://www.federalreserve.gov/supervisionreg/srletters/sr2115.htm.

[4] See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (April 1, 2022).

Board Internal Policies and Procedures

The Board has developed, documented, and implemented a comprehensive and robust agency-wide security program to protect the information and the information systems that support its operations and assets. The Board's information security program complies with federal information security requirements as established by FISMA and NIST standards and guidance issued in accordance with FISMA.

The Board's program includes technical, operational, and/or procedural controls to address access, telecommunications and network security, governance and risk management, software development, authentication and authorization, information security architecture and design, operations security, business continuity and disaster recovery planning, and physical (environmental) security that meet or exceed the standards established by FISMA. The Board's Office of Inspector General (OIG) performs an annual independent evaluation to determine the effectiveness of the Board's information security program and practices which includes an evaluation of the effectiveness of information security controls for select Board systems. Additionally, as part of the Board's continuous improvement approach to cybersecurity, the agency is currently engaged in efforts to enhance its cybersecurity lifecycle processes to support the Board's increasing reliance on cloud services, expand usage of multifactor authentication, and implement zero-trust architecture in accordance with the White House's "Executive Order on Improving the Nation's Cybersecurity."[10]

In addition to administering the agency's information security program, the Board also oversees the cyber-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 guidance and industry best practices. The Reserve Banks, as an operator of critical financial services, proactively provide tools and communications aimed at mitigating cyber 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, the Fedwire Securities Service, FedACH, and the National Settlement Service.[11] 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.

[10] See The White House, "Executive Order on Improving the Nation's Cybersecurity," last modified on May 12, 2021, https://www.whitehouse.gov/briefing-room/presidential-actions/2021/05/12/executive-order-on-improving-the-nations-cybersecurity/.

[11] See "Federal Reserve Banks Operating Circular No. 5 Electronic Access," effective June 30, 2021, https://www.frbservices.org/binaries/content/assets/crsocms/resources/rules-regulations/101520-operating-circular-5.pdf.

Board Activities to Address Cybersecurity Risks

The Board's activities help ensure the policies, procedures, rules, and guidance for supervised institutions and internal agency functions are successfully implemented. The Board's approach includes ensuring appropriate staffing, training, and resources for bank examiners. The Board also works with its OIG on continually improving cybersecurity supervisory activities and enhancing the Board's internal processes. Lastly, 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),[12] 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 cyber incidents and other hazards, safeguard critical infrastructure, and address emerging technology risks. The Federal Reserve examination staff use the *FFIEC IT Handbook*, which is informed by NIST standards and guidance along with other sources, in conducting cybersecurity and other technology-related examinations.

Examiners evaluate cybersecurity with consideration of the business model and activities conducted by supervised institutions as part of a principles-based supervision program. The scope of examinations is set as part of a multiyear supervisory plan that 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 or coordinated cyber reviews, with the OCC and FDIC. Additionally, for large financial institutions with assets of $100 billion or more,[13] the Federal Reserve conducts hori-

[12] U.S.C. §§ 1861-67.

[13] A LISCC firm is a firm that is supervised under the Large Institution Supervision Coordinating Committee supervisory program. Current LISCC 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. An 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 Large and Foreign Banking Organization supervisory program.

zontal cybersecurity examinations across institutions. Horizontal examinations promote consistency in the assessment of cyber governance and controls across firms, establish range of practice, and, as appropriate, allow the Federal Reserve to issue supervisory findings when weaknesses are present. In addition to the horizontal reviews, supervisory teams monitor cyber, IT, and operational risk using continuous monitoring processes as well as monthly engagement focused on emerging threats.

For community banking organizations (under $10 billion in assets) and regional banking organizations ($10 to $100 billion in assets), the Uniform Rating System for Information Technology (URSIT) is the primary mechanism to evaluate cybersecurity. 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 cyber threats.

For community banking organizations and regional banking organizations, the Board follows a risk-focused approach that assigns examination resources to higher-risk areas of each bank's operations and ensures that banks maintain risk-management capabilities appropriate to their size and complexity. Cybersecurity practices are evaluated with standardized procedures through regular information technology 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.

While the Board expects financial institutions to effectively manage risks associated with their third-party service providers, the BSCA provides authority for the federal banking agencies to regulate and examine certain services performed by third parties on behalf of insured depository institutions and their affiliates. The agencies jointly supervise a subset of third-party technology service providers through an interagency technology service provider supervision program, which incorporates a risk-based process for selecting service providers included in the program. For service providers in the program, through examinations, the agencies issue an URSIT rating which evaluates the condition of a service provider's information technology function. As part of the examinations, the agencies conduct cybersecurity specific examinations of these service providers which informs the firm's overall URSIT rating. The agencies 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 technology 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 super-

vised 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.[14]

For the FMU portfolio, the Board's Division of Reserve Bank Operations and Payment Systems works closely with staff at the New York and Chicago Reserve Banks, as well as at the Commodity Futures Trading Commission (CFTC) and Securities and Exchange Commission (SEC), to supervise designated FMUs' operational and cyber-risk management programs.[15] The Board regularly sets supervisory priorities for and examines (and 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 operational and cyber-risk management. Several PFMI standards that address cyber risk (including standards related to governance, operational risk, and comprehensive risk management), as well as the Cyber Resilience Guidance, provide common reference points for the three regulatory agencies in their supervision and oversight of the designated FMUs.

The Federal Reserve uses the ORSOM (Organization, Risk Management, Settlement, Operational Risk and Information Technology, and Market Support, Access, and Transparency) rating system in its assessment of designated FMUs. The rating system facilitates discussion of the FMU's condition with the FMU's management and board of directors. For a designated FMU for which the Board is the supervisory agency under title VIII of the Dodd-Frank Act, supervisory staff explain to the FMU the factors that determine that FMU's rating, including operational risks and information technology, which covers cyber risk.[17]

Furthermore, as part of our supervisory activities, the Federal Reserve has established processes and programs to monitor and share information involving cybersecurity threats, vulnerabilities, and incidents across the Federal Reserve System and the financial services sector. Additionally, the Federal Reserve monitors cybersecurity developments and events across the financial services sector including the payment, clearing, and settlement systems. The Federal Reserve proactively alerts examination staff to imminent cyber threats or vulnerabilities including ransomware, malware, and distributed denial of service (DDoS). These alerts provide examination staff the context to proceed with the appropriate Federal Reserve supervisory actions.

---

[14] Examples include Regulation P (12 C.F.R. pt.1016.) and the "red flags" rule under the Fair Credit Reporting Act (15 U.S.C. § 1681.).

[15] 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.

[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).

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

As discussed in table 1, federal banking regulatory agencies issued a rule[18] in November 2021 requiring banks to provide timely notification of serious cyber incidents. The implementation of this rule is being coordinated closely with both domestic and international partner agencies to maximize information sharing where possible, and to align expectations to minimize burden on reporting firms.

This rule will also complement a number of ongoing efforts. When a supervised institution experiences a cybersecurity incident, the Federal Reserve actively responds to evaluate the impacts of the incident on the firm, the financial sector, and payment systems. This consists of utilizing an assortment of tools, including an internal incident response network. This internal network helps facilitate other measures, such as sharing alerts with supervisory examiners.

Industry Efforts to Respond to 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 cyber risk.

When institutions do not address findings in an appropriate period of time, the Board has tools such as enforcement actions to ensure institutions operate in a safe and sound manner and safeguard critical infrastructure. The Board has observed improvement in cybersecurity practices over the past several years resulting from efforts to address supervisory findings as well as proactive steps taken by the institutions. However, continued vigilance from all parties is necessary.

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' cyber and information security practices, risk management, and controls to ensure that institutions implement appropriate and effective safeguards to mitigate cyber risk. For large domestic firms, using a risk-based approach, examiners are assigned to a specific firm or group of firms, and for foreign entities and smaller domestic institutions, examiners are assigned on a portfolio basis.

The Federal Reserve has established frameworks to direct the recruitment, hiring, and assignment of examiners, including IT and cybersecurity risk specialists. The Federal Reserve conducts training to ensure examiners remain prepared to address the latest threats to the financial ser-

[18] See Computer-Security Incident Notification Requirements for Banking Organizations and Their Bank Service Providers, 86 Fed. Reg. 66,424 (April 1, 2022).

vices sector and regularly updates its training program to ensure readiness to address current and prospective threats. The Federal Reserve has an online and mobile learning platform with an extensive catalogue of IT and information security training, which is available to all staff. The Federal Reserve has continued to assess cyber skills training and make incremental improvements. In addition, Federal Reserve examiners frequently participate in conferences and training events to gain perspective from external cybersecurity practitioners. The Federal Reserve has examiner affinity groups that serve as useful forums to share information and institutional knowledge of cyber resilience issues, including committees that address operational resilience matters across the portfolios supervised by the Federal Reserve.

Board OIG Efforts Related to Supervisory Activities

In 2017, the OIG conducted an evaluation to assess the Board's cybersecurity examination approach and to determine whether the Board was providing effective oversight of supervised institutions' information security controls and cybersecurity risk for select oversight areas.[19] As described in the last report to Congress, the Board is taking measures to address the OIG's recommendations, including reiterating to financial institutions the requirement under the BSCA to notify their primary regulator of the existence of new service relationships. The Federal Reserve, with other federal banking agencies, highlighted this requirement in connection with its proposed third-party risk management guidance, and is evaluating other options to improve compliance with this requirement.[20]

In 2020, the OIG issued a report identifying opportunities for the Board to enhance cybersecurity supervision of LISCC firms.[21] In response to the OIG's recommendation for more structured training, the Board created a formal interim training plan for LISCC cybersecurity examiners in 2021, as well as a new cybersecurity training plan that is applicable to examiners across the entire System beginning in 2022. These new training plans incorporate supervision, risk management, and technical cybersecurity skills as well as address emerging risks and best practices across the financial services sector.

Reserve Bank Activities

In addition to administering the Board's internal information security program, the Board also supervises the Reserve Banks' IT operations. The Reserve Banks continue to take measures to ensure they have robust protective measures for their critical operations. The Reserve Banks

---

[19] See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board Can Enhance Its Cybersecurity Supervision Approach in the Areas of Third-Party Service Provider Oversight, Resource Management, and Information Sharing* (Washington: Board of Governors, April 2017), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-apr2017.htm.

[20] 12 U.S.C. § 1867(c)(2).

[21] See Board of Governors of the Federal Reserve System, Office of Inspector General, *The Board's Approach to the Cybersecurity Supervision of LISCC Firms Continues to Evolve and Can Be Enhanced* (Washington: Board of Governors, September 2020), https://oig.federalreserve.gov/reports/board-cybersecurity-supervision-LISCC-firms-sept2020.htm.

remain vigilant about their cybersecurity posture, investing in risk-mitigation initiatives and programs and continuously monitoring and assessing cybersecurity risks to operations and protecting systems and data. The Reserve Banks continue to implement cybersecurity initiatives to enhance identity and access management capabilities; enhance the ability to respond to evolving cybersecurity threats with agility, decisiveness, and speed by streamlining decision-making during a cybersecurity incident; and improve continuous monitoring capabilities of critical assets. Additionally, in light of recent increases in ransomware activity in the financial sector, the Reserve Banks have taken actions to strengthen processes, infrastructure, and controls to further enhance ransomware protections and response capabilities consistent with CISA and FBI guidance on mitigating ransomware risks.

The Reserve Banks have also focused their efforts on bolstering the security of the U.S. payment system. For example, in 2021, the Reserve Banks implemented a new FedACH processing platform to improve the efficiency and reliability of FedACH operations. The Reserve Banks also continue to enhance the resiliency and information security posture of the Fedwire Funds, National Settlement Service, and Fedwire Securities Service through a multiyear initiative to respond to environmental threats and cyber threats.

Additionally, the Reserve Banks maintain an information security program for FedLine Solutions, which provides financial institutions direct electronic access to the Reserve Banks' payment services.[22] As part of this program, financial institutions that use FedLine Solutions must conduct an annual assessment of their compliance with the Reserve Banks' FedLine security requirements and submit an attestation that they have completed the assessment. To the extent any deficiencies or gaps are identified in the self-assessment, institutions must develop a remediation plan to address such deficiencies.

Coordination Activities

Due to the high degree of interconnectedness of the global financial system, the Board is an active participant and leader in domestic and international forums addressing the cyber resiliency of the financial services sector. The Board closely coordinates 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 services sector and reduce the effects of cyber-related incidents, the Board coordinates with partners through the President's

[22] See "Assurance Program Frequently Asked Questions," Federal Reserve Bank Services, https://www.frbservices.org/resources/fedline-solutions/faq/fedline-assurance-program.html.

Working Group on Financial Markets (PWGFM), the Financial and Banking Information Infrastructure Committee (FBIIC), and the Federal Financial Institutions Examination Council (FFIEC).

The Board is a member of the PWGFM, whose mission is 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 cyber and other operational risks. Most recently, the Board has actively contributed to the group's initiatives studying cyber vulnerabilities across the financial services sector and emerging technologies such as stablecoins.[23]

The Board is also a member of FBIIC, which is chartered under the PWGFM. FBIIC is composed 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 coordinates and shares information with respect to security issues that may influence the financial services sector and has established protocols to respond to incidents affecting institutions supervised by FBIIC members. In the past year, FBIIC has engaged on a number of areas relating to cybersecurity, including third-party risk management, supply chain security, and incident response.

The Board participates in FBIIC's periodic cyber exercises that include participation from the regulatory agencies, financial institutions, and trade associations. 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 cyber resiliency. These include an initiative to enable participating financial institutions to store critical customer account data in a secure industry-standard format, and capabilities to proactively identify, analyze, and coordinate activities to mitigate systemic risk to the U.S. financial system (and other critical infrastructure) from cyber 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 FFIEC members on cybersecurity risk-management issues. The Board contributes to the efforts of the FFIEC in responding to cyber incidents affecting institutions supervised by FFIEC members. The Board also contributes to the FFIEC's efforts and supports ongoing dialogue on cybersecurity issues and opportunities to improve consistency in examination approaches.

[23] See U.S. Department of the Treasury, "President's Working Group on Financial Markets Releases Report and Recommendations on Stablecoins," news release, November 1, 2021, https://home.treasury.gov/news/press-releases/jy0454.

Public and Private Sector Coordination

The Board participates in various 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 cyber 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.

Through FBIIC, the Board also coordinates with the Financial Services Sector Coordinating Council (FSSCC), a nonprofit body composed of over 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 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 2022, joint FBIIC and FSSCC priorities include the protection of supervisory data, cyber exercises, and cyber workforce development.

One important example of this type of coordination is the "Hamilton Series." For this initiative, FS-ISAC partners with the FSSCC, the Treasury, and other U.S. government agencies, including law enforcement, to develop one-day, simulated exercises aimed at improving responses to a range of cyber-threat scenarios within the U.S. financial sector. Participants include members of both the public and private sectors, and exercise outcomes contribute to improved public and private coordination strategies.

International Coordination

The Board leads or contributes to 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).

In light of the threat cyber incidents pose to the global financial system, the FSB has assumed a key role in promoting cybersecurity risk-management standards. To that end, the FSB in October 2020 published a toolkit to provide financial institutions with a set of effective practices to respond to and recover from a cyber incident to limit any related financial stability risks. In October 2021, the FSB published a report identifying ways to achieve greater convergence in cyber incident reporting to facilitate information-sharing across jurisdictions and sectors.[24]

[24] See Financial Stability Board, "FSB Calls for Greater Convergence in Cyber Incident Reporting," news release, October 19, 2021, https://www.fsb.org/2021/10/fsb-calls-for-greater-convergence-in-cyber-incident-reporting/.

The BCBS acts as the primary global standard setter for the prudential regulation of banks and provides a forum for cooperation on banking supervisory matters. The Board's deputy director of Supervision and Regulation currently serves as the chair of the BCBS Operational Resilience Group (ORG). In March 2021, the BCBS issued the Principles for Operational Resilience[25] and the Principles for the Sound Management of Operational Risk, which the ORG was charged with drafting.[26] These documents highlight the importance of sound operational risk management, including cyber-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 cyber threats, intended to complement earlier actions and promote widespread adoption of measures to strengthen banks' cybersecurity.[28]

Through the CPMI-IOSCO, the Board has played a key role in the development of the PFMI and related guidance for FMIs, including the Cyber Resilience Guidance. The CPMI-IOSCO Working Group on Cyber Resilience has promoted implementation of the guidance across member jurisdictions and engaged with private sector firms to better understand operational risks and cybersecurity risk management.

The Board contributed to the development of IAIS's key financial stability priorities for insurance providers in November 2021. Among these was a focus on increasing cyber risk, which is increasingly creates significant impacts to insurers' financial liabilities. In 2021, the Board contributed to the first full global monitoring exercise conducted by the IAIS to assess global insurance market trends and developments and detect the possible build-up of systemic risk in the global insurance sector, including heightened cyber risk.[29]

Given the rapidly evolving nature of cyber risks and the cross-border and cross-sector relevance of cyber threats, the G-7 finance ministers, central bank governors, and other financial authorities established a working group consisting of cybersecurity experts to elevate cybersecurity concerns and enhance cooperation among G-7 jurisdictions and the financial services sector. The G-7 cyber working group has published papers on cybersecurity topics, including a paper calling for common categorizations of malicious cyber incidents and other operational IT incidents to aid in comparing

---

[25] See Basel Committee on Banking Supervision, *Principles for Operational Resilience* (Basel: 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* (Basel: Bank for International Settlements, March 2021), https://www.bis.org/bcbs/publ/d515.pdf.

[27] See SR 20-24 letter.

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

[29] See International Association of Insurance Providers, "IAIS Global Monitoring Exercise (GME) Highlights Key Financial Stability Priorities for Insurance Supervisors," news release, November 30, 2021, https://www.iaisweb.org/uploads/2022/01/211130-IAIS-Press-Release-GIMAR-2021.pdf.

and studying incidents across jurisdictions.[30] Current G-7 cyber priorities include coordinating responses to ransomware, cyber events across jurisdictions, and cyber risks from third-party service providers and emerging technologies.

Board Internal

The Board promotes effective cybersecurity risk management through active collaboration and coordination across Board functions and stakeholders. The Board's Office of the Chief Operating Officer (OCOO) facilitates the efficient and timely exchange of critical information regarding cyber risk issues across business, IT, and information security functions, and supports the coordination of cross-functional perspectives among Board stakeholders on cyber policy issues. This collaboration includes discussion and analysis of current and emerging threats and incidents.

The Board maintains a vigilant cybersecurity posture, investing in risk-mitigation initiatives and programs, protecting systems and data, and continuously monitoring and assessing cybersecurity risks to our operations. The Board's information security program, which complies with federal information security requirements as established by FISMA and NIST standards and guidance, includes protection of information assets against advanced persistent threats (APTs), malware, insider risks, DDoS attacks, and other risks. These protections are provided in a layered approach to provide interlocking prevention, detection, response, remediation, and recovery capabilities as described below.

At the preventive layer, the Board has deployed technologies such as firewall, proxy, and application gateway on the perimeter to manage access to and from the Board's network. Preventative capabilities are enhanced by incorporating threat intelligence from the public and private sectors. In addition, users are required to complete annual security awareness training and policies and best practices are periodically highlighted for staff in posts on the Board's intranet. The Board also regularly conducts phishing exercises to raise awareness among users. Users who fail the exercises are required to complete phishing awareness training.

With respect to detection, the Board leverages a comprehensive security information and event management platform that ingests and indexes log data from various network and endpoint sources for correlation, including, but not limited to, telemetry from the prevention technologies noted above. In addition to log data, the Board leverages various technologies to actively analyze email and web traffic to detect potential malicious content.

[30] See Cyber Expert Group, "Proposal for a Common Categorisation of IT Incidents," April 6, 2021, https://acpr.banque-france.fr/sites/default/files/medias/documents/20210406_occasional_paper_categorisation_incidents.pdf.

With respect to response, the Board has an experienced team of incident responders that monitor and investigate any suspicious activity on the Board's network. If suspicious activity is determined to be malicious, a cyber incident notification and escalation process is followed. In the event an incident requires additional resources beyond the capabilities of the Board's incident response team, the Board has an established relationship with the larger Federal Reserve System incident response team to provide assistance, as needed. The Board also has a retainer agreement with an external incident response service provider to provide additional expertise and surge capacity as needed.

As response efforts transition to remediation, the Board has subject matter experts that can be leveraged to assist with remediation efforts on various technologies deployed throughout the enterprise. For use cases where the remediation is driven by patching vulnerabilities, the Board has a robust patch management program that includes the regular scanning of its environment for vulnerabilities. Furthermore, the Board works with the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) to leverage its offering to regularly scan external-facing web assets for vulnerabilities and corresponding remediation. Similarly, the Board established a vulnerability disclosure policy pursuant to Binding Operational Directive 20-01 for these externally facing web assets.

As an incident moves to the recovery stage, the Board has established a multi-layered approach. For IT services, such as email, that require high availability, the Board has established "hot" duplicate services that can be leveraged with minimal business disruption. In addition, a "warm" contingency remote site is maintained which includes data backups. These backups support the Board's ability to recover services in a timely manner.

The Board continues to be mindful of the need to regularly assess the maturity, efficacy, and readiness of various technologies and capabilities described above as it relates to the Board's overall cybersecurity posture. To that end, the Board regularly assesses its cybersecurity posture via a combination of self-initiated activities, such as annual compromise assessments, annual penetration tests, annual data exfiltration exercises, and tabletop exercises. As a result, the Board continues to mature and evolve its cybersecurity capabilities.

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 FISMA, DHS publishes FISMA reporting metrics. These metrics direct IGs to evaluate the effectiveness of agency information security programs across various attributes

grouped into eight security domains.[31] These domains align with the five security functions defined by the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework): *identify, protect, detect, respond, and recover*.[32] Pursuant to the FISMA reporting metrics, IGs assess the effectiveness of each of the five NIST Cybersecurity Framework function areas 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 as operating at an effective level of security. The Board OIG's 2021 assessment of the Board's overall information security program rated the program as continuing to operate effectively at a level 4 maturity.[33]

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

The Board takes a continuous improvement approach to strengthening its information security program across the five NIST Cybersecurity Framework function areas. The Board's chief information security officer (CISO) manages a Plan of Actions and Milestones process that ensures plans are developed in response to any finding or weakness identified in security and privacy control implementations. This process is used to track and report on the remediation of findings and implementation recommendations issued by the OIG and weaknesses identified through internal testing of controls.

The Board's CISO coordinates with members of the FFIEC and with CISA in response to cybersecurity directives. The CISO reports directly to CISA and the Office of Management and Budget regarding cybersecurity directives and executive orders. Lastly, the CISO is continually working to improve the Board's information security program and may establish tactical and strategic initiatives to enhance existing cybersecurity and privacy processes.

The CISO serves a critical role assessing risk and acting in the best interest of the agency by eliminating threats. The Board's information security and IT staff continually monitor for new threats and vulnerabilities that may be identified and communicated by cybersecurity researchers, vendors, information sharing and analysis centers, and CISA. The CISO leads any response to cyber threats and vulnerabilities identified by CISA and require remediation. Informal consultation

---

[31] See "FY 2020 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics, Version 4.0," Cybersecurity and Infrastructure Security Agency, last modified on April 17, 2020, https://www.cisa.gov/sites/default/files/publications/FY_2020_IG_FISMA_Metrics.pdf.

[32] See "Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1," National Institute of Standards and Technology, April 16, 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP04162018.pdf. The NIST Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise.

[33] See Board of Governors of the Federal Reserve System, Office of Inspector General, *2020 Audit of the Board's Information Security Program* (Washington: Board of Governors, November 2020), https://oig.federalreserve.gov/reports/board-information-security-program-nov2020.pdf.

and benchmarking on key cybersecurity issues is conducted with other regulatory agencies including the FFIEC agencies.

Russia's invasion of Ukraine, which has involved cyberattacks on Ukrainian government and critical infrastructure organizations, may affect entities both within and beyond the region. In response, CISA and its Joint Cyber Defense Collaborative (JCDC) partners have responded to ongoing, disruptive cyber activities in connection with Russia's attack by documenting information on Russian threat actors, ransomware, destructive malware, and DDoS attacks, and by promoting "Shields Up" protective measures. These measures include remediating vulnerabilities, enforcing Multi-Factor Authentication, using antivirus, enabling strong spam filters to prevent phishing emails from reaching end users, disabling ports and protocols that are not essential, and strengthening controls for cloud services. The Board has and continues to review its technical controls and security processes against the "Shields Up" recommendations. These efforts include exercising our controls against known Russian cyberattack techniques and methods and enhancing our controls through efforts like the implementation of a zero-trust architecture.

Current or Emerging Threats to Financial System Resilience

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

The rising number of advanced persistent threats increases the potential for malicious cyber activity within the financial sector. These threats may result in incidents that affect one or more participants in the financial services sector simultaneously and 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.

One well-known threat-type is traditional ransomware. The proliferation of ransomware poses a threat to the operational and financial resilience of all institutions but may disproportionately affect small community and regional banking organizations that may not have sufficient resources to protect their systems against sophisticated actors.

In addition to traditional ransomware, other sophisticated capabilities may also pose a risk to financial institutions' ability to operate and protect customer data.

- **Ransomware as a service (RaaS)**. Like traditional ransomware, ransomware as a service (RaaS) is an increasing concern with added sophistication, speed of proliferation, and difficulty of attribution. RaaS allows threat actors to create "franchised" threat offerings. Sophisticated threat actors license the use of their software to other malicious actors, often for a percentage of the ransom. This evolving threat model allows less sophisticated threat actors greater opportunity to impact businesses. Organizations that refuse to pay the ransom often need to rebuild infrastructure to restore business operations.
- **Sophisticated DDoS threats.** Sophisticated DDoS threats, in which the perpetrator seeks to make a machine or network resource unavailable to its intended users by overwhelming the target or its surrounding infrastructure with disruptive traffic, also continue to be an area of concern. DDoS attempts against the U.S. financial services sector have been prevalent for years, but mitigation and protection services are typically able to prevent, or greatly reduce, the risk to financial institutions, third parties, and other organizations.

In addition to these threat types, the enhanced connectivity of cyber threat organizations is an additional area of concern. With such connectivity, threat actors are increasingly sharing information relating to vulnerabilities that may be exploited. The increase in information sharing among different threat actors is an emerging concern because it reduces the window of opportunity to prevent incidents once a vulnerability is discovered.

There are a number of ways that threat actors utilize the threat types described above. One of the most common methods utilizes existing vulnerabilities in software. Vulnerabilities continue to provide malicious cyber actors an opportunity to exploit susceptible systems, whether the vulnerabilities are known to the public or not. Sophisticated cyber groups may seek to develop "zero-day" exploits, which take advantage of unknown vulnerabilities, while others will attempt to rapidly exploit new, publicly disclosed vulnerabilities before victims apply published fixes.

In addition to these concerns, there are a number of newly emerging threats that offer threat actors new incentives, attack vectors, and opportunities to exploit vulnerabilities in technology.

Increasing Geopolitical Tensions

Geopolitical events, such as the Russian invasion of Ukraine, have led to the potential for increase in cyberattacks that may impact critical infrastructure including the financial services sector. Given the evolving threat landscape and potential for exploitation of vulnerabilities, domestic financial institutions have maintained a heightened state of preparedness. The Board and other federal banking agencies are closely monitoring developments related to this threat. Thus far, there have not been material impacts to financial sector cybersecurity in relation to this threat.

Increasing Potential of a Supply Chain or Third-Party Attack

A significant evolving risk is the impact of a cyberattack at a vendor or third party. Coupled with the threat types described above, supply chain compromise can impact the financial system through legitimate connections with third-party service providers. Software-as-a-service relies on an ongoing connection between a software provider and a client firm, where the product is remotely updated on a periodic basis. The ability of threat actors to breach software providers and subsequently use the breached provider's software to compromise the provider's client firms highlights the risks stemming from interdependency often associated with third-party vendor management and automated software updates being applied. As third-party software, and software-as-a-service, in particular, becomes increasingly common in banking, these risks are multiplied.

Other Emerging Technology-Related Threats

Potential cybersecurity vulnerabilities in fintech applications; such as cryptocurrency exchanges, banking applications; or other platforms offer threat actors an opportunity to steal funds or data by compromising victims' computer systems or technology infrastructure used to interact with the products or services. For example, control of digital assets often depends on the safeguarding of private keys tied to the underlying asset. Accordingly, threat actors who obtain unauthorized access to the private keys may take control of the underlying asset with little recourse for the victim. Another example of emerging technology-related risk is data sharing between financial institutions and third-party financial technology service providers, where financial institutions allow service providers access to financial data to build applications and services around the financial institution. These arrangements offer consumers the potential for access to new or better services, but such arrangements also provide greater opportunity for malicious actors to gain access to private data. In general, fintech platforms continue to offer users new digital products and services, but such emerging technologies are often vulnerable to exploitation by tech savvy hackers looking to profit from technical and financial vulnerabilities in these technologies.

Threats such as these highlight the importance of the Board and Federal Reserve System efforts outlined in this report. Cyber-risk mitigation and cyber 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 cyber threats, the Federal Reserve continues to maintain a strong internal resilience posture and promote resilience among the financial sector as a whole.

Find other Federal Reserve Board publications (www.federalreserve.gov/publications.htm) or order those offered in print (www.federalreserve.gov/files/orderform.pdf) on our website. Also visit the site for more information about the Board and to learn how to stay connected with us on social media.

www.federalreserve.gov
0722