Cybersecurity Resources for Community Banks

This is a voluntary resource providing a non-exclusive compilation of publicly available content for convenience and informational purposes only. The Federal Reserve neither endorses the information, content, presentation, or accuracy nor makes any warranty, expressed or implied, regarding the organizations sponsoring linked websites and does not endorse the views they express or the products or services they offer. This resource does not have the force or effect of law and does not prescribe any specific practices or standards nor establish any safe harbors for compliance with laws or regulations. While it is intended for use by community banks, other banks may find it useful.

POTENTIAL SOURCES OF INFORMATION

Federal Financial Institutions Examination Council (FFIEC)

FFIEC members are taking a number of initiatives to raise the awareness of financial institutions and their third-party service providers with respect to cybersecurity risks and the need to identify, assess, and mitigate these risks in light of the increasing volume and sophistication of cyber threats.

Content: The referenced resource guides and alerts pertain to cybersecurity awareness and various joint agency statements and can be found at www.ffiec.gov/.

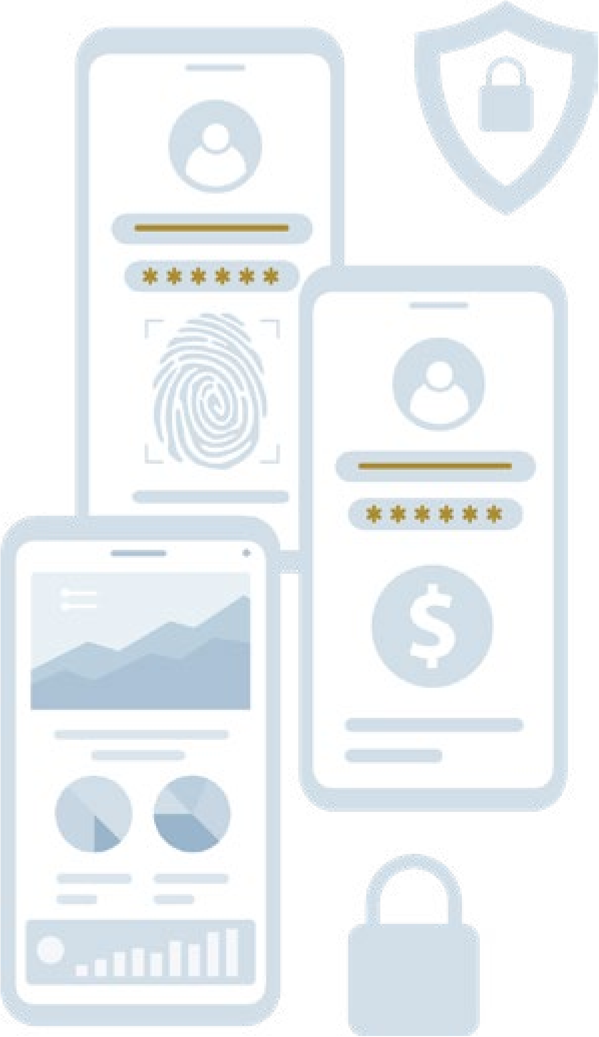
Notifications: Sign up for alerts at www.ffiec.gov/.

FFIEC resources related to cybersecurity:

- Cybersecurity Awareness Webpage
- Cybersecurity Assessment Tool Sunset Statement
- FFIEC Cybersecurity Resource Guide for Financial Institutions
- FFIEC Statement on Security in a Cloud Computing Environment
- FFIEC IT Examination Handbook

United States Treasury's Project Fortress

U.S. Department of the Treasury established Project Fortress to improve the security and resilience of the financial services sector through forward-leaning public-private information sharing mechanisms. Project Fortress includes a mix of proactive defensive and offensive measures to help secure the financial sector. For more information, please see https://home.treasury.gov/.



Cybersecurity Infrastructure and Security Agency (CISA)

CISA is the operational lead for federal cybersecurity and the national coordinator for critical infrastructure security and resilience. CISA is designed for collaboration and partnership with a mission to reduce risk to the nation's cyber and physical infrastructure.

Content: The programs and services offered by CISA seek to help organizations better manage risk and increase resilience using all available resources.

Notifications: Sign up for alerts at www.cisa.gov.

CISA cybersecurity resources and services available at www.cisa.gov:

- Cyber Hygiene Services
- Free Cybersecurity Services and Tools
- Tabletop Exercise Packages

CYBERSECURITY SELF-ASSESSMENT TOOLS

National Institute of Standards and Technology (NIST)

NIST is part of the U.S. Department of Commerce. NIST developed the Cybersecurity Framework, which provides guidance to industry, government agencies, and other organizations to manage cybersecurity risks.

The Cybersecurity Framework is available at www.nist.gov/cyberframework.

Center for Internet Security (CIS)

CIS is an independent, nonprofit organization. CIS developed the Critical Security Controls (CIS Controls) as a prescriptive, prioritized, and simplified set of cybersecurity posture best practices.

CIS Controls are available at www.cisecurity.org/controls.

CISA

CISA developed the Cross-Sector Cybersecurity Performance Goals (CPGs), which are a subset of cybersecurity practices, selected through a thorough process of industry, government, and expert consultation, aimed at meaningfully reducing risks to both critical infrastructure operations and the American people. Financial Services Sector-Specific Goals are expected to be released soon.

CISA CPGs are available at www.cisa.gov/cross-sector-cybersecurity-performance-goals.

Cyber Risk Institute (CRI)

CRI is a not-for-profit coalition of financial institutions and trade associations. CRI developed the Cyber Profile as a global standard for cyber risk assessment. It consists of a list of assessment questions based on the intersection of global regulations and cyber standards, such as the International Organization for Standardization and NIST.

The Cyber Profile is available at https://cyberriskinstitute.org/the-profile/.

FEDERAL RESERVE

Supervision and Regulation Letters

Supervision and Regulation (SR) letters address significant policy and procedural matters related to the Federal Reserve System's supervisory responsibilities.

Content: SR letters cover a variety of topics including: information technology guidance, information technology examination process, cybersecurity, business continuity/disaster recovery, and operational resilience.

Notifications: Active SR letters are available at www.federalreserve.gov/supervisionreg/srletters/srletters.htm. Additionally, topical supervisory policy and guidance is located on the Information Technology Guidance webpage.

SR letters related to cybersecurity:

- SR 24-7: FFIEC Cybersecurity Assessment Tool Sunset Statement
- SR 22-4: Contact Information in Relation to Computer-Security Incident Notification Requirements
- SR 21-14: Authentication and Access to Financial Institution Services and Systems
- SR 05-23: Interagency Guidance on Response Programs for Unauthorized Access to Customer Information and Customer Notice
- SR 01-15: Standards for Safeguarding Customer Information

Federal Reserve webpages of interest:

- Operational Resilience, at www.federalreserve.gov/supervisionreg/topics/operational-resilience.htm.
- Cybersecurity and Operational Resilience, at www.federalreserve.gov/supervisionreg/cybersecurity-and-operational-resilience.htm.

Community Banking Connections

Community Banking Connections is a source for information on guidance, resources, and tools that help community banks across the United States.

Content: Information technology, information security, and cybersecurity are often covered. Articles on these topics can be found at www.communitybankingconnections.org/topical-index.

Notifications: Sign up to receive notifications at www.communitybankingconnections.org.

***Community Banking Connections* articles related to cybersecurity:**

- Security in the Cloud: A Discussion with the Regulators
- 2024 Midwest Cyber Workshop Recap
- Ransomware: A Multifaceted Menace
- Ransomware Defense: A Discussion with the Regulators
- Endpoint Security: On the Frontline of Cyber Risk
- Maintaining Strong Cybersecurity Controls Is Imperative as Online Threats Increase
- Notifying Primary Federal Regulators About Computer-Security Incidents

Ask the Fed

Ask the Fed is a program for officials of banks and bankers' associations to address new or important regulatory issues or supervisory guidance.

Content: Sessions can be viewed at https://bsr.stlouisfed.org/askthefed. For past information technology content, select the "All Calls" tab.

Notifications: Register for an account on the Ask the Fed site, then opt in to communications under "My Account."

Ask the Fed sessions related to cybersecurity:

- Sunset of the FFIEC CAT Session 2: A Discussion with the Cyber Risk Institute (CRI) (April 2025)
- Sunset of the FFIEC CAT Session 1: A Discussion with the Center for Internet Security (CIS) (March 2025)
- Insights with the Cybersecurity and Infrastructure Security Agency (CISA) Part II (December 2024)
- Insights with the Cybersecurity and Infrastructure Security Agency (CISA) (February 2024)
- Maturing Your IT Risk Management and Governance Framework (December 2022)
- Ask the Regulators: Computer-Security Incident Notification Rule (April 2022)
- For more information about Ask the Fed: Questions@AsktheFed.org

The Supervision Contact System

The Supervision Contact System (SCS) is used by the Federal Reserve Bank (FRB) supervision functions to communicate Board of Governors supervisory guidance and other information in a timely manner to the financial institutions they supervise.

Content: SCS is used primarily to distribute information needed by financial institutions within the scope of the FRB's supervision. Such regulatory information includes SR letters, Consumer Affairs letters, and other supervisory guidance.

Notifications: Individuals from supervised institutions create a profile on the SCS website (a secure website hosted by the FRB of St. Louis) at https://supervisioncontactsystem.org and follow the prompts on https://Login.gov.*

If you have any questions, please contact the SCS Support Center at: 855-727-5919 or supervision.contact@stls.frb.org.

The Emergency Communications System

The Emergency Communications System (ECS) is a free service that is a means for state supervisory agencies and FRB supervision functions to communicate with financial institutions they regulate in an emergency situation.

Content: ECS is only used to contact institutions during real emergencies and during semiannual tests. The following situations might necessitate the use of ECS:

- Natural disasters
- Man-made disasters: Chemical biological events or threats
- Events affecting the financial markets
- Cyber events

Notifications: Individuals from supervised institutions create a profile on the ECS website (a secure website hosted by the Federal Reserve Bank of St. Louis) at https://bsr.stlouisfed.org/ecs and follow the prompts on https://Login.gov.*

If you have any questions, please contact the ECS Support Center at: 855-327-5333 or ecs.support@stls.frb.org.

LAW ENFORCEMENT CONTACT INFORMATION

Federal Bureau of Investigation

The Federal Bureau of Investigation (FBI) has 55 field offices (also called divisions) centrally located in major metropolitan areas across the United States and Puerto Rico. Field offices carry out investigations, assess local and regional crime threats, and work closely with partners on cases and operations.

Find a field office near you at www.fbi.gov/contact-us/field-offices.

The United States Secret Service

With local field offices across the United States, the Secret Service also has a Cyber Fraud Task Force staffed with special agents, technical experts, and forensic analysts.

Find a field office near you at www.secretservice.gov/contact/field-offices.

*Institutions should add Frb.org and Stls.frb.org email domains to their safe-sender list to ensure receipt of SCS and ECS communications.