Office of the Comptroller of the Currency

Report on Cybersecurity and Resilience of the Federal Banking System

Office of the Comptroller of the Currency
Washington, D.C.

July 2021

Contents

Preface

The Consolidated Appropriations Act, 2021 (CAA)[1] requires the Office of the Comptroller of the Currency (OCC) to issue an annual report to Congress for the next seven years describing measures the OCC has taken to strengthen cybersecurity with respect to the agency's functions as a regulator. Functions include the supervision and regulation of financial institutions and, when applicable, third-party service providers.

As required by the CAA, this report addresses

- an analysis of the OCC's internal cybersecurity policies and procedures adopted in accordance with the Federal Information Security Modernization Act (FISMA) of 2014.
- a description of the OCC's policies and procedures that guard against
  - efforts to deny access to or degrade, disrupt, or destroy information and communications technology systems or networks, or exfiltrate information from such a system or network without authorization.
  - destructive malware attacks.
  - denial of service activities.
  - other efforts that may threaten the functions of the OCC or OCC-supervised entities by undermining cybersecurity and the resilience of the financial system.
- a description of the activities the OCC has undertaken to ensure the effective implementation of the policies and procedures described above, including
  - the appointment of qualified staff, the provision of staff training, the use of accountability measures to support staff performance, and the designation, if any, of senior appointed leadership to strengthen accountability for oversight of cybersecurity measures within the OCC and among OCC-supervised entities.
  - deployment of adequate resources and technologies.
  - efforts to respond to cybersecurity-related findings and recommendations of the OCC's inspector general or the independent evaluation described under the Federal Information Security Modernization Act.
  - industry efforts to respond to cybersecurity-related findings and recommendations of the banking regulators.
  - efforts to strengthen cybersecurity in coordination with other federal agencies, domestic and foreign financial institutions, and other partners, including the development and dissemination of best practices regarding cybersecurity and the sharing of threat information.
  - a description of current and emerging threats likely to pose a risk to the resilience of the financial system.

[1] Refer to Pub. L. No. 116-260, Division Q, Section 108.

Executive Summary

The OCC charters, regulates, and supervises national banks and federal savings associations and licenses, regulates, and supervises federal branches and agencies of foreign banking organizations.[2] As of the OCC's September 30, 2020, fiscal year end, the federal banking system comprised 1,158 banks operating in the United States. These banks range from small community banks to the largest and most globally active U.S. banks. In total, the banks within the federal banking system held $14.1 trillion of all assets of U.S. commercial banks (68 percent of the total assets held by all U.S. commercial banks).[3]

In addition, the OCC examines services performed on behalf of banks by certain third parties under the authorities conferred by the Bank Service Company Act and Home Owners' Loan Act.[4] Examination of service providers is conducted in coordination with the Board of Governors of the Federal Reserve System (Federal Reserve) and the Federal Deposit Insurance Corporation (FDIC).

The OCC views cybersecurity and operational resilience as top issues for the federal banking system and has reiterated this in the fiscal year 2021 Bank Supervision Operating Plan by making them key priorities for supervisory strategies.[5] Cyber attacks continue to compromise security of technology systems, affect operations, and result in breaches of sensitive information across all sectors, including banking. Cyber attacks become more sophisticated and damaging each year. Recent publications of the OCC's *Semiannual Risk Perspective* emphasize the importance of banks continuing to strengthen their risk posture and remaining vigilant of malicious actors' efforts to circumvent cybersecurity controls.[6]

This report discusses actions the OCC is taking to address heightened cybersecurity and resilience risks as part of supervisory processes and efforts to maintain the security and integrity of OCC internal systems and information assets. Key highlights include:

- key regulations, supervisory guidance, examination manuals, and other publications that the OCC has developed on its own and with other agencies to communicate supervisory expectations and effective practices for cybersecurity and resilience.
- supervisory processes and banks' efforts to implement and maintain effective cybersecurity and resilience risk management practices and controls to safeguard against current and emerging threats.
- internal cybersecurity policies, practices, and controls to safeguard the OCC's sensitive information and sensitive information that the agency has collected.

[2] This report refers to all entities under OCC supervision collectively as "banks" unless it is necessary to distinguish among them.

[3] Refer to the OCC's *2020 Annual Report*.

[4] Refer to 12 USC 1867(c) and 1464(d)(7).

[5] Refer to OCC News Release 2020-130, "OCC Releases Bank Supervision Operating Plan for Fiscal Year 2021."

[6] Refer to the OCC's *Semiannual Risk Perspective*, May 18, 2021.

- views on cybersecurity and resilience threats to the federal banking system and efforts to communicate and share information with regulatory counterparts and the banking industry.

The OCC is committed to providing effective oversight and supervision of the federal banking system for cybersecurity preparedness and resilience and ensuring effective cybersecurity controls and practices for the agency. As part of these efforts, the OCC closely collaborate with the agency's domestic regulatory partners, international colleagues, and industry stakeholders.

Policies and Procedures to Safeguard Against Cybersecurity Threats

Oversight of OCC-Supervised Banks

The OCC issues regulations governing the safe and sound operations of banks. In addition, the OCC issues guidance and other information to communicate effective practices related to cybersecurity. The OCC also issues examination manuals for examiners related to the agency's supervisory activities.[7] This section describes regulations, supervisory guidance and resources, and examination manuals related to the OCC's oversight of cybersecurity and resilience risks in the federal banking system.

Cybersecurity-Related Regulations

The OCC has implemented a number of regulations and safety and soundness standards that require banks to implement appropriate information security programs and to protect confidential information. For example:

- **Safety and soundness standards**: The "Interagency Guidelines Establishing Standards For Safety and Soundness Standards" at 12 CFR 30, appendix A, set out the safety and soundness standards the OCC uses to identify and address problems at insured depository institutions before capital becomes impaired. The "Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches" at 12 CFR 30, appendix D, establish minimum standards for the design and implementation of a covered bank's risk governance framework and board of directors' oversight. Together, the aforementioned guidelines require banks to have internal controls and information systems appropriate for the size of the institution and for 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 OCC's safety and soundness standards also require banks to have internal audit systems that provide for adequate testing and review of information systems.
- **Safeguarding sensitive customer information**: Pursuant to Title V, Subtitle A, of the Gramm–Leach–Bliley Act,[8] the OCC implemented regulations requiring banks to establish appropriate administrative, technical, and physical controls for the safeguarding of customer information. Working with the other federal banking agencies, the OCC published these standards as 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standard." These interagency guidelines require banks to implement information security programs to ensure the security and confidentiality of customer information; protect against any anticipated threats or hazards to the security or integrity of such information; protect against unauthorized access to or use of such information that could result in

[7] Refer to, e.g., *Comptroller's Handbook* and the *Federal Financial Institutions Examination Council's Information Technology Examination Handbook*.

[8] Refer to 15 USC 6801–6809.

substantial harm or inconvenience to any customer; and ensure the proper disposal of customer and consumer information.

- **Suspicious activity reporting**: OCC regulations require banks to file Suspicious Activity Reports when banks detect a known or suspected violation of federal law or a suspicious transaction related to a money laundering activity or a violation of the Bank Secrecy Act.[9] This includes expectations for reporting certain computer crimes.

Incident Notification Notice of Proposed Rulemaking

The OCC, FDIC, and Federal Reserve published a notice of proposed rulemaking (NPR) that would require a covered entity to provide its primary federal regulator with prompt notification of any "computer-security incident" that rises to the level of a "notification incident," as defined in the NPR. The deadline for comments on the proposed rule was April 12, 2021.[10] The agencies are considering issues and concerns that commenters raised on the proposal and are working to develop a final rule.

Supervisory Guidance and Resources

The OCC publishes, on its own and in conjunction with other regulatory agencies, supervisory guidance and other documents to help banks understand supervisory expectations, increase awareness of cybersecurity risks, and assess and mitigate risks. Recent examples of cybersecurity-related supervisory guidance and other documents include

- "Sound Practices to Strengthen Operational Resilience"[11]
- "Joint Statement on Security in a Cloud Computing Environment"[12]
- "Joint Statement on Heightened Cybersecurity Risk"[13]

Many cybersecurity publications and resources have been coordinated through the Federal Financial Institutions Examination Council (FFIEC). The FFIEC members have published a number of cybersecurity-related resources, including the cybersecurity assessment tool (CAT) published June 30, 2015. The FFIEC CAT provides a repeatable, measurable process for banks to assess their cybersecurity preparedness over time. The CAT incorporates cybersecurity-related principles from the *FFIEC Information Technology Examination Handbook,* existing supervisory guidance, and concepts from industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework.

[9] Refer to 12 CFR 21.11 and 163.180.

[10] Refer to OCC Bulletin 2021-3, "Computer-Security Incident Notification: Notice of Proposed Rulemaking."

[11] Refer to OCC Bulletin 2020-94, "Operational Risk: Sound Practices to Strengthen Operational Resilience."

[12] Refer to OCC Bulletin 2020-46, "Cybersecurity: Joint Statement on Security in a Cloud Computing Environment."

[13] Refer to OCC Bulletin 2020-5, "Cybersecurity: Joint Statement on Heightened Cybersecurity Risk."

Additional FFIEC resources include industry outreach, examiner webinars, and the "Cyber Security Resource Guide," which provides resources designed to assist financial institutions with cybersecurity preparedness and resilience. These documents and resources can be accessed on the FFIEC Cybersecurity Awareness web page.

Appendix A of this report provides a list of key cybersecurity-related supervisory guidance statements and other resources published by the OCC and our regulatory partners from 2015 to present.

Examination Manuals

The OCC oversees the federal banking system by implementing and enforcing federal banking law and maintaining a supervisory and regulatory framework that encourages banks to innovate and adapt to meet the evolving financial needs of consumers, businesses, and communities nationwide.[14] The OCC uses a risk-based supervision process focused on evaluating banks' risk management, identifying material and emerging concerns, and requiring banks to take corrective action when warranted. The supervision process is outlined in the *Comptroller's Handbook.*[15]

The OCC uses the FFIEC's Uniform Rating System for Information Technology (URSIT) to assess information technology (IT) risks at financial institutions, their affiliates, and service providers to identify those institutions that require special supervisory attention. The URSIT framework includes elements to assess information security and other risk management factors to determine the quality, integrity, and reliability of the bank's or third-party service provider's IT.[16]

For detailed IT information and work programs, OCC examiners use the *FFIEC Information Technology Examination Handbook*. It comprises a series of booklets addressing IT-related supervision topics. The booklets include examination work programs. Aspects of cybersecurity are included in various booklets, such as "Management," "Information Security," "Business Continuity Management," and "Outsourcing Technology Services."[17] These booklets are updated periodically, with the most recent update being the June 30, 2021, publication of the "Architecture, Infrastructure and Operations" booklet.[18]

Appendix B of this report provides a list of key technology- and cybersecurity-related examination manuals published by the OCC individually and through the FFIEC.

---

[14] Refer to the OCC's *2020 Annual Report*, p. 1.

[15] Refer to, e.g., "Bank Supervision Process" booklet of the *Comptroller's Handbook.*

[16] Refer to the "Uniform Rating System for Information Technology" section of the "Bank Supervision Process" booklet of the *Comptroller's Handbook*.

[17] The booklets are on the FFIEC IT Examination Handbook Infobase.

[18] Refer to OCC Bulletin 2021-30, "FFIEC Information Technology Examination Handbook: New Architecture, Infrastructure, and Operations Booklet."

Outreach Efforts

The OCC regularly engages in outreach efforts to engage with banks and other stakeholder to communicate cybersecurity and resilience risks and best practices through a number of forums. The OCC regularly hosts outreach meetings for supervised banks and will structure certain meetings for key bank roles, such as board members, chief executive officers, chief risk officers, and chief information and information security officer roles to better structure content, including topics related to cybersecurity and resilience. Additionally, OCC subject matter experts will speak at industry sponsored forums on cybersecurity, resilience, and other IT related topics to communicate key risks and best practices.

OCC Internal Security

The OCC operates a comprehensive information security and cyber protection program to protect the information and information systems that support its operations and assets, including the sensitive financial institution information in the agency's custody. The program includes:

- policies, standards, and controls that meet or exceed requirements established by FISMA and related issuances from the Office of Management and Budget, the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), and the NIST.
- 24/7/365 cyber defense operations and technologies.
- 24/7/365 incident response capabilities.
- a cross-functional data breach response team that complements incident response capabilities by providing management oversight and support to evaluate actual or suspected data loss events and guide the agency's response to such events.
- information assurance processes in the OCC's system development and acquisition life cycle.
- continuous monitoring and assessment of security and privacy control effectiveness.

The OCC operates full life cycle incident prevention, detection, disruption, and response processes, including

- configuration and operation of intrusion prevention and detection, advanced persistent threat detection, endpoint malware prevention and detection, and data loss prevention technologies;
- threat intelligence services employing industry and federal sources; and
- operation of an enterprise logging infrastructure for continuous monitoring of all network traffic and event correlation for the discovery of anomalous cyber activity across the network and its end-hosts.

The OCC maintains and routinely exercises disaster recovery, continuity of operations, and information system contingency plans to ensure that effective resources and procedures are in place to enable recovery and reconstitution of critical agency functions and supporting information systems in response to disrupted or diminished service conditions.

Implementation of Cybersecurity Policies and Procedures

The OCC's bank supervision and the agency's own internal governance focus on (1) maintaining fundamental security risk management practices and controls to safeguard against cyber threats and (2) emphasizing the importance of effective response programs and operational resilience capabilities to mitigate and limit the impact in the event of a cybersecurity breach. The OCC published its supervisory priorities in its Fiscal Year 2021 Bank Supervision Operating Plan to provide the foundation for policy initiatives and supervisory strategies for individual banks, listing cybersecurity and operational resilience as top priorities.[19]

Oversight of OCC-Supervised Banks

Staffing and Resources

As of the OCC's September 30, 2020, fiscal year end, the OCC had approximately 2,250 bank examiners.[20] Safety and soundness examiners receive training on fundamental cybersecurity and overall information technology supervision. The OCC has an internal training and development curriculum for examiners, which includes bank IT courses that incorporate cybersecurity concepts. These courses are supplemented with specific training on emerging issues, such as ransomware. All safety and soundness examiners receive sufficient training to conduct IT and cybersecurity examinations at non-complex community banks.

In addition to generalist examiners, the OCC has a cadre of IT specialist examiners who are subject matter experts and focus on complex supervisory issues related to technology operations, including cybersecurity. Many of these specialists hold industry certifications such as ISACA's Certified Information Systems Auditor or the ISC² Certified Information Systems Security Professional.[21] IT specialist examiners regularly attend industry conferences and more advanced external training to gain further expertise on IT and cybersecurity topics.

Examiners are generally assigned to the Large Bank Supervision (LBS) department, which includes banks that generally have assets between $50 billion and $3 trillion, or the Midsize and Community Bank Supervision (MCBS) department. Within MCBS, examiners can be assigned to Midsize Bank Supervision or one of the OCC's four districts responsible for community bank supervision. Midsize Bank Supervision generally includes banks with assets between $8 billion and $60 billion and the four districts supervise community banks under $8 billion in assets that typically conduct traditional banking activities.

In addition to bank examiners in the MCBS and LBS departments, the OCC has additional supervision and subject matter expert resources that support cybersecurity oversight and supervision. The following are some examples.

---

[19] Refer to OCC News Release 2020-130, "OCC Releases Bank Supervision Operating Plan for Fiscal Year 2021."

[20] Refer to the OCC's 2020 Annual Report.

[21] See CISSP's Cybersecurity Certification page.

- The Systemic Risk Identification Support & Specialty Supervision (SyRIS) division identifies, evaluates, and holistically addresses risks that affect the OCC's mission, provides subject matter expertise across all risk disciplines, assists in resource prioritization focusing on the highest risk financial institutions and companies, and provides direct supervision to special purpose charters[22] and service providers. SyRIS has a unit of subject matter experts focused on information technology risks, including cybersecurity, and the Significant Service Provider supervision team that is dedicated to the examination of large and complex technology service providers.
- The Bank Supervision Policy department maintains two policy units that focus on cybersecurity and resilience risks. The first is the Bank Information Technology Policy unit that develops and maintains supervisory guidance, resources, examination manuals, and supervisory tools that help examiners carry out cybersecurity supervision. The second is the department's Critical Infrastructure Policy unit, which identifies and assesses systemic operational risks that could degrade or interrupt the federal banking system. The Critical Infrastructure Policy unit also supports the coordination of internal responses and information sharing during critical infrastructure events, such as cybersecurity incidents.[23]
- The Office of Innovation, also part of the Bank Supervision Policy department, is the central contact and clearinghouse for requests and information relating to innovation in the federal banking system. This unit coordinates OCC outreach and engagement with banks and financial technology companies on new or innovative products, services, and technologies being considered or implemented in the federal banking system. This unit also coordinates issues related to cybersecurity and resilience.

Bank Supervision Activities

The OCC conducts full-scope examinations of each bank every 12 to 18 months depending on the bank's characteristics, such as asset size and financial condition.[24] The 12- to 18-month full-scope examination frequency is referred to as the supervisory cycle. Statutory and regulatory requirements generally set the maximum supervisory cycle length but do not limit the OCC's

[22] Special purpose banks generally offer a small number of products, target a limited customer base, incorporate nontraditional elements, or have narrowly targeted business plans. Examples of special purpose banks include trust banks, community development banks, and credit card banks. For more information, refer to the "Special Purpose Banks" section of the "Bank Supervision Process" booklet of the *Comptroller's Handbook* and the "Charters" booklet of the *Comptroller's Licensing Manual*.

[23] The Bank Supervision Policy department provides timely information, analysis, policy guidance, and examination procedures, and encourages an OCC culture receptive to responsible innovation. The department also supports examiners, OCC senior management, and other OCC stakeholders on emerging risk and supervisory issues confronting the financial system and federal banks and collaborates with domestic and international regulators.

[24] The OCC examines banks pursuant to the authority conferred by 12 USC 481, 1463, and 1464, as well as the requirements of 12 USC 1820(d). The OCC examines federal branches and agencies pursuant to the authority conferred by 12 USC 3105(c)(1)(C). In addition, 12 USC 1820(d) requires the OCC to conduct a full-scope examination of each insured depository institution every 12 or 18 months. The OCC applies this statutory requirement to all types of banks (federal branches and agencies excepted), regardless of FDIC-insured status, in 12 CFR 4.6. The frequency of full-scope examinations for federal branches and agencies is prescribed by 12 USC 3105(c) and 12 CFR 4.7. For more information, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook*.

authority to examine a bank as frequently as the OCC deems appropriate.[25] As part of every supervisory cycle, the OCC conducts an IT assessment for each bank that includes an examination of cybersecurity activities.

The supervisory strategy is the OCC's detailed supervisory plan for each bank, which outlines supervisory objectives, activities, and work plans. Strategies are developed for each supervisory cycle and updated as needed throughout. Strategies define the goals of supervision for a specific bank based on its risk profile, and they are the foundation for supervisory activities and work plans to be conducted during the supervisory cycle. Examinations of specific areas, such as IT and cybersecurity, are conducted as part of a full-scope or targeted examination. Key aspects of the supervisory process related to cybersecurity include:

- **IT rating**: Examiners assess a bank's ability to identify, measure, monitor, and control IT risks related to information security, business continuity planning, audit, systems development, outsourcing, and other assessment factors outlined in the URSIT. In addition, examiners assess compliance with 12 CFR 30, appendix B, "Interagency Guidelines Establishing Information Security Standards." Examiners complete an IT core assessment for each bank during every supervisory cycle.[26] The *FFIEC Information Technology Examination Handbook* contains detailed work programs that supplement the core assessment.
- **Risk assessment system:** The OCC's risk assessment system (RAS) is a concise method of communicating and documenting conclusions regarding eight risk categories: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. Examiners draw conclusions regarding the quantity of risk, quality of risk management, aggregate risk, and direction of risk for each of the eight categories. Examiners consider the results of IT assessments when drawing RAS conclusions for relevant risk categories, such as operational, compliance, strategic, and reputation.[27]
- **FFIEC CAT**: OCC examiners have incorporated the FFIEC CAT in examinations since 2016. Use of this tool has allowed the OCC to implement a consistent cybersecurity supervision framework. The CAT also enables the OCC to monitor cybersecurity preparedness across the federal banking system. By using this tool over several supervisory cycles, examiners have been able to observe the range of practices across banks, identify common areas of strength and potential control gaps, and better measure the level of preparedness across banks over time.
- **Ongoing supervision:** Ongoing supervision is the OCC's process for assessing risks and reviewing core knowledge about a bank on an ongoing basis. Ongoing supervision conclusions can result in changes to the OCC's supervisory strategy, regulatory ratings, or RAS conclusions for a bank.

[25] A potential or actual adverse change in a bank's condition or risk profile, a change in bank control, or an OCC scheduling conflict are examples of when the OCC may determine that it would be appropriate to examine the bank more frequently.

[26] Refer to the "Community Bank Supervision," "Federal Branches and Agencies Supervision," and "Large Bank Supervision" booklets of the *Comptroller's Handbook.*

[27] For more information, refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook.*

- **Other resources**: Examiners use cybersecurity concepts that are communicated in or through the supervisory publications, such as the *FFIEC Information Technology Examination Handbook,* but also use other resources, for example,
  - NIST Cybersecurity Framework and alerts issued from organizations. These include the DHS CISA to help inform supervision oversight.
  - Center for Internet Security Critical Security Controls.
  - Cyber Risk Institute's Financial Sector Cybersecurity Profile.[28]
- **Communication of examination findings**: As part of the supervision process, the OCC is committed to ongoing, effective communication with supervised banks. Communication includes formal and informal conversations, scheduled meetings, issuance of supervisory letters, reports of examination, and other written communication. Communication is ongoing throughout the supervisory process and tailored to a bank's structure and dynamics; the timing and form depend on the situation being addressed. Results of OCC examinations are communicated to a bank's board and management through reports of examination and supervisory letters.
- **Deficient practices**: When examiners identify deficient practices,[29] the OCC takes appropriate supervisory action to require a bank to take corrective action. The primary vehicle used to communicate supervisory concerns to a bank's board and management is in the form of matters requiring attention (MRA). Examiners cite violations of laws and regulations in writing. Violations, deficient practices, or unsafe or unsound practices also may serve as the basis for an enforcement action. Formal enforcement actions are public and may include Cease-and-Desist Orders, Civil Money Penalty Orders, and other actions. The OCC conducts periodic follow-up of a bank's corrective actions in response to MRAs, violations, and enforcement actions.[30]

Interagency Supervision Activities

The OCC actively coordinates with the FDIC and Federal Reserve on cybersecurity and resilience supervision for significant organizations within the banking sector. One example of this coordination is the interagency coordinated cybersecurity review program. It is designed to align and improve the efficiency of cybersecurity supervision at the largest and most systemically important financial institutions through better examination coordination and resource use by federal banking regulators. By coordinating their reviews of the largest banking organizations, the agencies can better focus on the areas of highest cybersecurity risk to the federal banking system, increases efficiencies in the use of cybersecurity supervision subject matter experts across the agencies, and provide for more effective supervision of highly complex organizations.

---

[28] Refer to Center for Internet Security's CIS Controls and Cyber Risk Institute's The Profile

[29] A deficient practice is a practice, or lack of practices, that
- deviates from sound governance, internal control, or risk management principles and has the potential to adversely affect the bank's condition, including financial performance or risk profile, if not addressed, or
- results in substantive noncompliance with laws or regulations, enforcement actions, or conditions imposed in writing in connection with the approval of any applications or other requests by the bank.

[30] Refer to the "Bank Supervision Process" booklet of the *Comptroller's Handbook.*

Another example of where the agencies closely coordinate is the examination of significant third-party service providers to supervised banks. Service providers can pose a significant risk to their bank clients and to the banking system if the providers have operational or financial issues that affect the delivery of critical services. These examinations are typically conducted jointly by the OCC, FDIC, and Federal Reserve, and when applicable, with the participation of state banking regulators. The "Supervision of Technology Service Providers" booklet of the *FFIEC Information Technology Examination Handbook* includes an overview of the service provider examination program. Key aspects of the service provider examination program include the following:

- Service providers are identified for examination using several factors, such as the criticality of services provided, number of banking institutions serviced, and total assets serviced.
- Examinations typically focus on services such as core banking services (e.g., loans, deposits, and balance sheet activities), payment services, technology infrastructure services, mortgage processing, and trust services.
- Examination activities for service providers follow interagency guidelines[31] and use the *FFIEC Information Technology Examination Handbook* and other applicable guidance.
- Annual strategies are developed for service provider examination activities. The strategies define supervisory goals for a specific service provider based on its risk profile, including cybersecurity-related activities.
- The OCC, FDIC, and Federal Reserve have implemented a consistent framework for cybersecurity assessments for technology service providers, based on the FFIEC CAT.

Similar to supervision of banks, reports of examination are issued for service providers, and, when appropriate, MRAs are used to communicate concerns with deficient practices. Reports of examination are made available to client financial institutions receiving contracted services.

Bank's Efforts to Respond to Cybersecurity and Resilience Concerns

Cybersecurity and technology management continue to be key areas of supervisory concern. Although banks have made significant investments in their security programs, continuous vigilance is required to adapt to the changing cyber threat landscape. Banks have been responsive to identified cybersecurity concerns; however, cybersecurity threats continue to evolve and opportunities remain for further improvement.

The *Semiannual Risk Perspective* regularly highlights cybersecurity as a risk. The fall 2019[32] report featured cybersecurity as a special topic and highlighted that while many MRAs focus on general policy and security program governance issues, the most common cybersecurity control deficiencies relate to the following areas:

[31] Refer to *Implementation of Interagency Programs for the Supervision of Technology Service Providers*, October 31, 2012.

[32] Refer to OCC Highlights Key Risks for Federal Banking System.

- **Access management:** Excessive or inappropriate access rights can provide malicious actors with unauthorized access and lead to compromised systems and bank or customer data. Ineffective authentication controls can heighten this risk.
- **Patch management:** Challenges with identification, risk rating, testing, and implementing system patches and updates on a timely basis.
- **Network configuration:** Misconfigured security settings on firewalls and network control devices or other system misconfigurations can create security gaps, thus allowing malicious actors to gain access to banks' internal networks to remove sensitive data or conduct unauthorized transactions.

The OCC maintains formal processes for tracking and following up on a bank's corrective actions in response to MRAs, violations, and enforcement actions. MRAs, violations and enforcement actions are closed when examiners have verified and validated the bank's corrective actions.

To better identify and address the root cause of issues before they become concerns, examiners are focusing on banks implementation of strong authentication programs, appropriate use of data encryption, effective inventory management of technology assets, strong system configuration standards, and appropriate security tools that identify and mitigate malicious attacks. Banks are expected to maintain appropriate risk management processes to continually test and validate the effectiveness of these controls, including thorough network vulnerability assessments and penetration testing, as well as processes to ensure that corrective actions are made in a timely manner.

Recent *Semiannual Risk Perspective* reports have also highlighted the key role that banks' third-party relationships can have on cybersecurity and resilience. Effective risk management for critical third-party relationships is essential for safe and sound operations. The OCC, Federal Reserve, and FDIC issued a request for comment on proposed interagency guidance on risk management for third-party relationships on July 19, 2021.[33] This update of existing third-party risk management guidance includes key considerations for security and resilience when engaging third parties.

Efforts to Respond to Independent Reviews of OCC Supervision

The OCC is subject to oversight by the U.S. Department of the Treasury's Office of the Inspector General (OIG) and the Government Accountability Office (GAO). The OCC has been subject to several inspections related to cybersecurity, either directly or as part of broader financial agency reviews. The OCC has been responsive to all independent assessments and implemented corrective actions for recommendations addressed to the agency. All OIG and GAO audit reports are available for review on their respective websites.

[33] Refer to OCC Bulletin 2021-31, "Third-Party Relationships: Notice and Request for Comment on Proposed Interagency Guidance."

Domestic and International Coordination on Cybersecurity

The OCC coordinates with a number of domestic and international organizations to share cyber threat information, communicate effective cybersecurity practices, and align cybersecurity efforts. In addition to the direct interagency coordination efforts already outlined in this report, one of the key vehicles for coordination is the FFIEC.[34] Through the FFIEC's Task Force on Supervision, groups such as the Cybersecurity and Critical Infrastructure Working Group and the Information Technology Subcommittee have developed and published a wide range of documents and resources for assessing cybersecurity risks.

The OCC also actively coordinates with the Treasury Department's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) and the broader financial sector regulatory agencies through participation on the Financial and Banking Information Infrastructure Committee (FBIIC).[35] The FBIIC, chaired by the Treasury Department, was chartered under the President's Working Group on Financial Markets and comprises 18 federal and state financial services regulatory agencies or organizations that provide supervision of the banking, investment, and insurance subsectors. The FBIIC helps to coordinate interagency efforts to improve the reliability and security of the financial sector infrastructure by sharing threat information and effective security practices and coordinating responses to cybersecurity and other significant events that affect the financial sector.

In addition to coordinating with domestic regulatory counterparts, the OCC also engages with industry groups. The OCC engages with the Financial Services Sector Coordinating Council (FSSCC), through the FBIIC, to coordinate on such topics such as sector-wide cyber exercises, training, information sharing, situational awareness, and incident communication and coordination. The OCC plays an active role in regularly scheduled joint FBIIC/FSSCC meetings. This partnership is fully articulated in the *Financial Services Sector-Specific Plan 2015*.

Additionally, the OCC coordinates regularly with the Financial Services Information Sharing and Analysis Center (FS-ISAC) and Analysis and Resilience Center (ARC) for threat and vulnerability monitoring and resilience efforts. The FFIEC members issued a statement[36] encouraging financial institutions to join and engage with FS-ISAC to increase participation and coordination. When appropriate, the OCC engages bilaterally with law enforcement and other government agencies regarding threat information or specific issues affecting financial institutions.

An example of this coordination includes the Hamilton series exercises developed by private sector groups, the Treasury Department, and other relevant U.S. government agencies to simulate an assortment of cyber or other resilience events affecting the financial sector to improve public

[34] The FFIEC, established in 1979, comprises the Office of the Comptroller of the Currency, the Board of Governors of the Federal Reserve System, Federal Deposit Insurance Corporation, National Credit Union Administration, Consumer Financial Protection Bureau, and the State Liaison Committee.

[35] Refer to the FBIIC's web page.

[36] Refer to FFIEC Press Release, "FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center."

and private sector coordination. A key outcome resulting from the exercise program is Sheltered Harbor, a voluntary industry initiative for data vaulting to safeguard critical data in the event of a destructive malware attack.[37] The OCC issued an interagency statement noting that institutions should consider whether their backup and restoration practices are consistent with industry standards and frameworks, including Sheltered Harbor.[38]

The OCC regularly engages banking supervisory authorities internationally on cybersecurity and operational resilience-related matters. Examples of such engagement include serving as a member on the Basel Committee on Banking Supervision (BCBS) and participating as an observer with the Financial Stability Board (FSB). These groups work to establish common principles across jurisdictions on key issues facing the global financial system. Recent publications from these groups include BCBS's *Principles for Operational Resilience* (March 31, 2021) and FSB's *Effective Practices for Cyber Incident Response and Recovery* (October 19, 2020).

Appendix C of this report highlights key domestic and international groups that the OCC collaborates with on cybersecurity- and resilience-related matters.

OCC Internal Security

The OCC Chief Information Security and Chief Privacy Officer (CISO) is designated by the OCC Chief Information Officer (CIO) to carry out the CIO's responsibilities under FISMA. OCC hiring procedures for the CISO is designed to ensure that this individual possesses the requisite professional qualifications and has the singular mission focus to execute these responsibilities. The OCC CISO develops and leads the OCC's Information Security and Cyber Protection program and serves as director for the OCC Cyber Security Office (CSO), a division of the CIO's organization with the mission and resources to help the agency manage its information and cybersecurity risks. CSO key program areas include Cyber Security Operations, Cyber Security Readiness, Cyber Assurance and Compliance, Data Privacy and Security, Cyber Policy, and Disaster Recovery. Individual development plans for CSO staff members target professional certifications and skills development along with CISO/CPO priorities in domains of interest, such as cloud security. In accordance with the Federal Cybersecurity Workforce Assessment Act of 2015, the National Initiative for Cybersecurity Education coding structure is applied to position descriptions involving cybersecurity responsibilities to ensure that proper qualifications are required for these positions.

The OCC Information Security and Cyber Protection program spans the agency offices, programs, operations, and processes required to protect OCC information and information systems against threats to their confidentiality, integrity, and availability. The CSO delivers ongoing agency-wide awareness and training for the OCC end-user community to ensure that all agency personnel understand their program responsibilities and their individual accountability for their actions regarding these responsibilities. For several years this awareness and training effort has focused on five key cybersecurity risks associated with end-user behavior:

[37] See "Sheltered Harbor's Mission."

[38] See OCC Bulletin 2020-5, "Cybersecurity: Joint Statement on Heightened Cybersecurity Risk."

unauthorized release of sensitive information; malware infection of a computer or device; loss of OCC-issued IT equipment or personal identity verification credential; unencrypted email transmission of personally identifiable information; and a successful phishing attempt. Regular phishing exercises and routine information security bulletins target behavior improvements, and ongoing tracking and reporting to management encourages individual accountability for performance.

Senior appointed leadership at the OCC is limited to the Comptroller, who signs the agency head letter to meet FISMA's annual reporting requirement. The Comptroller, OCC Senior Deputy Comptrollers (SDC), and the OCC Chief Risk Officer (CRO) receive monthly cybersecurity/privacy briefings and ad hoc briefs from the CISO. SDCs serve as authorizing officials for OCC information systems and serve on senior executive subcommittees focusing on technology investment and enterprise risk management.

Adequate resources and technologies for executing the OCC's Information Security and Cyber Protection program are allocated using a risk-based approach that integrates OCC budget activities with the CIO's Work Intake & Solution Evaluation and Capacity Based Operating Plan processes, and the senior executive subcommittee focusing on technology investment. This approach prioritizes capital investment projects associated with higher risk to the agency based on its enterprise risk appetite statement, including technology and reputation risks associated with information security. Cybersecurity status and major investments are reported to the technology investment subcommittee, which includes the CRO, who reports directly to the Comptroller.

Consistent with FISMA requirements, the OCC engages resources through the Treasury Department's OIG to conduct an annual evaluation of the Information Security and Cyber Protection program. The OCC achieved a Level 4 maturity rating in the OIG's fiscal year 2020 FISMA audit and has maintained a "Managing Risk" rating for its performance on quarterly CIO FISMA metrics. The OCC received important assurance in March 2021 from an independent assessment by a leading cybersecurity service confirming no instances of any advanced persistent threat.

CSO manages a Plan of Actions and Milestones process that ensures that these plans are developed in response to any findings or weaknesses identified in security and privacy control implementation. This process is used to track and report on the remediation of findings and implementation of recommendations when issued by the OIG in response to its evaluation of the OCC Information Security and Cyber Protection program and supporting practices.

The OCC's cybersecurity coordination with other federal agencies centers on its responsibility as an independent regulatory agency to report directly to CISA in response to cybersecurity directives and tasks. The OCC ensures that all CISA reporting is shared with the Treasury Department's security operations center to facilitate cross-departmental information sharing and collaboration on cyber threats and vulnerabilities. Informal consultation and benchmarking on key cybersecurity issues is conducted with other regulatory agencies and member agencies of FIFIEC.

Current and Emerging Cybersecurity Threats

Oversight of Supervised Institutions

Cybersecurity Threat Information Sharing

The OCC actively monitors for emerging threats through the supervisory process, engagement with federal partners, and monitoring sector alerts. The OCC's Critical Infrastructure Policy unit is responsible for the identifying and assessing systemic operational risk that could degrade or interrupt the federal banking system and lead to national economic security concerns. As part of these efforts, the Critical Infrastructure Policy unit regularly monitors FS-ISAC, Homeland Security Information Network, Financial Crimes Enforcement Network, and other open-source, cyber-related information feeds to maintain situational awareness of evolving financial sector risks. OCC supervision teams respond to reports of security incidents and operational outages that occur at supervised institutions and monitor trends to assess emerging risks.

The OCC encourages banks to engage with and monitor threat notices and alerts from FS-ISAC, CISA, and other similar threat information-sharing forums to receive timely and actionable threat information. When appropriate, the OCC directly shares alert information, often with interagency counterparts, through internal communication channels to reinforce its importance and emphasize risk mitigation.

The OCC actively engages in sharing information with financial regulators to coordinate assessments and response. The Treasury Department is the Sector Risk Management Agency for the financial services sector and the OCC coordinates with OCCIP and other FBIIC members on cybersecurity and critical infrastructure matters. The OCC participates in monthly FBIIC classified meetings where threat and vulnerability information is conveyed by the Treasury Department and other federal agencies, such as DHS, and intelligence community agencies and partners. When identifying and responding to cyber threats and vulnerabilities affecting financial institutions, the OCC engages with federal law enforcement and other agencies as needed for support.

Current and Emerging Cybersecurity Threats

The OCC has multiple mechanisms to identify and measure current and emerging risks to the banking sector. One of the key groups focusing on this analysis is the National Risk Committee. Committee members include senior agency officials who supervise banks of all sizes and develop bank supervisory policy. The National Risk Committee monitors the condition of the federal banking system and identifies key risks and emerging threats to the system's safety and soundness and ability to provide fair access to financial services and treat customers fairly. Current and emerging cybersecurity and resilience threats to the banking sector that the OCC has been most focused on include:

- **Ransomware:** The frequency and severity of ransomware attacks continue to increase targeting organizations of all sizes, including those in the financial sector. Malicious actors continue to pressure organizations to pay extortion demands in exchange for decrypting

sensitive data that have been encrypted or to prevent the release of sensitive information obtained during a cyber attack.

- **Account takeover:** Cyber criminals have used a number of ways to gain unauthorized access, or otherwise take over, customer accounts. These attacks are becoming more sophisticated but still often rely on phishing to gain initial access and stolen credentials to perpetuate fraud. Stolen customer credentials may give an attacker access to customers' account information to commit fraud and identity theft. Stolen employee and third-party credentials may provide initial access to trusted internal systems. Similarly, business email compromise and similar tactics are used to send fraudulent payment instructions to financial institutions or other business associates, or to effect financial fraud. These schemes continue to grow and adversely affect financial institutions and their customers.
- **Supply chain risks:** Cyber criminals are increasingly exploiting vulnerabilities in widely used IT systems and services to conduct malicious cyber activities. In supply chain attacks, software designed to help maintain clients' systems and networks, is compromised and used to spread malicious software, affecting thousands of customers. Victims of these attacks have included government agencies, financial sector entities, and technology service providers. Recent high-profile incidents demonstrate the need for banks to assess the risks emanating from their suppliers and third parties and to develop a comprehensive cooperative approach to operational resilience.

Although additional threats persist in the banking sector, these supply chain attacks have had significant impact and are increasing. These threats are communicated to OCC-supervised banks, service providers, and other stakeholders through a number of channels, including the OCC's *Semiannual Risk Perspective*. The *Semiannual Risk Perspective* addresses key issues facing banks, focusing on those that pose threats to the safety and soundness of banks and their compliance with applicable laws and regulations; the report also has highlighted cybersecurity and resilience as key risks to the industry.

OCC resources also monitor longer-term technology developments, which may affect cybersecurity and resilience in the future. These emerging developments and technological advances can both strengthen security or create new cybersecurity risks as malicious actors seek to exploit them. OCC subject matter experts, including Office of Innovation staff, monitor these longer-term developments and engage with stakeholders to assess their potential impact on the financial sector. A recent example of these efforts is the interagency request for information on financial institutions' use of artificial intelligence, including machine learning.[39] This request included questions on how the use of artificial intelligence technologies may impact cybersecurity.

OCC Internal Security

CSO's threat intelligence team continually monitors industry and federal threat intelligence sources, including CISA and FS-ISAC, to identify emerging threats to the agency. Every month, the CISO/CPO briefs the Comptroller and members of the Executive Committee, including the CRO, on current cybersecurity threats to the OCC identified by CSO's 24/7/365 Cyber Defense

[39] Refer to OCC Bulletin 2021-17, "Artificial Intelligence: Request for Information on Financial Institutions' Use of Artificial Intelligence, Including Machine Learning."

Center. The OCC's Enterprise Risk Committee, which is chaired by the CRO and comprises senior agency leadership, continues to highlight cybersecurity as a key risk for the OCC as an organization. Threat trends include targeted phishing campaigns, ransomware, and unauthorized access attempts by nation-state actors.

Appendixes

Appendix A: Cybersecurity Supervisory Guidance and Resources (2015–Present)

Organization	Date	Document Type	Title	Description
OCC/Federal Reserve/FDIC	July 19, 2021	Policy for comment	Third-Party Relationships: Notice and Request for Comment on Proposed Interagency Guidance	The proposed interagency guidance is based on the OCC's existing third-party risk management guidance from 2013. The proposed interagency guidance would replace each agency's existing guidance on this topic and would be directed to all banking organizations supervised by the agencies
OCC, Federal Reserve, FDIC	January 12, 2021	Policy for comment	Notice of Proposed Rulemaking: Computer-Security Incident Notification	Notice of proposed rulemaking requirements that would require a banking organization to provide its primary federal regulator with prompt notification of any ''computer-security incident'' that rises to the level of a ''notification incident.''
OCC, Federal Reserve, FDIC	October 30, 2020	Sound practices	Sound Practices to Strengthen Operational Resilience	Guidance that provides firms with ways to strengthen their operational resilience in the face of internal and external operational risks that, left unchecked, could lead to a wide-scale disruption.
FFIEC	April 30, 2020	Joint statement	Security in a Cloud Computing Environment	Statement to address the use of cloud computing services and security risk management principles in the financial services sector.
OCC, FDIC	January 16, 2020	Joint statement	Heightened Cybersecurity Risk	Statement to reiterate to supervised financial institutions sound cybersecurity risk management principles.
FFIEC	November 5, 2018	Joint statement	Office of Foreign Assets Control Cyber-Related Sanctions Program Risk Management	Statement to alert financial institutions to recent actions taken by the Treasury Department's Office of Foreign Assets Control (OFAC) under OFAC's Cyber Related Sanctions Program and to the potential impact that sanctions may have on financial institutions' operations, including the use of services of a sanctioned entity.
FFIEC	October 2018	Resource guide	FFIEC Cybersecurity Resource Guide	The resource guide provides resources designed to assist in financial sector information data and security resilience.
FFIEC	April 10, 2018	Joint statement	Cyber Insurance and Its Potential Role in Risk Management Programs	Statement to provide awareness of the potential role of cyber insurance in financial institutions' risk management programs.

Organization	Date	Document Type	Title	Description
FFIEC	May 2017	Assessment Tool	Cybersecurity Assessment Tool	The Cybersecurity Assessment Tool (CAT) provides a repeatable and measurable process to measure their cybersecurity preparedness over time. The CAT incorporates cybersecurity-related principles from the *FFIEC Information Technology Examination Handbook,* regulatory guidance, and concepts from other industry standards, including the NIST Cybersecurity Framework. Using the CAT is voluntary for financial institutions. The OCC has incorporated its use into the agency's supervision program.
FFIEC	June 7, 2016	Joint statement	Cybersecurity of Interbank Messaging and Wholesale Payment Networks	Reminder to financial institutions of the need to actively manage the risks associated with interbank messaging and wholesale payment networks.
FFIEC	November 2015	Joint statement	Cyber Attacks Involving Extortion	Statement to notify financial institutions of the increasing frequency and severity of cyber attacks involving extortion.
FFIEC	March 30, 2015	Joint statement	Destructive Malware	Statement to notify financial institutions of the increasing threat of cyber attacks involving destructive malware.
FFIEC	March 30, 2015	Joint statement	Cyber Attacks Compromising Credentials	Statement to financial institutions about the growing trend of cyber attacks for the purpose of obtaining online credentials for theft, fraud, or business disruption and to recommend risk mitigation techniques.
FFIEC	November 3, 2014	Joint statement	Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement	Statement recommending that participating in information-sharing forums is an important element of an institution's risk management processes and its ability to identify, respond to, and mitigate cybersecurity threats and incidents.

Appendix B: Key Examination Booklets

Organization	Title	Description
OCC	*Comptroller's Handbook*	The OCC *Comptroller's Handbook* is prepared for use by OCC examiners in connection with their examination and supervision of national banks, federal savings associations, and federal branches and federal agencies of foreign banking organizations (collectively, banks). Each bank is different and may present specific issues. Accordingly, examiners should apply the information in the booklets consistent with each bank's individual circumstances. Topics covered are • Examination Process • Safety and Soundness – Capital Adequacy – Asset Quality – Management – Earnings – Liquidity – Sensitivity to Market Risk – Other Activities • Asset Management • Consumer Compliance • Securities Compliance
FFIEC	*FFIEC Information Technology Examination Handbook*	The FFIEC members developed the *FFIEC Information Technology Examination Handbook* using a principles-based approach to IT risk management. The handbook comprises 11 booklets addressing the following topics: • Architecture, Infrastructure, and Operations • Audit • Business Continuity Management • Development and Acquisition • E-Banking • Information Security • Management • Outsourcing Technology Services • Retail Payment Systems • Supervision of Technology Service Providers • Wholesale Payment Systems

Appendix C: Examples of Domestic and International Interagency Organizations the OCC Participates With

Organization	Key Cybersecurity-Related Subgroups	Description
Federal Financial Institutions Examination Council	Task Force on Supervision: • Information Technology Subcommittee • Cybersecurity and Critical Infrastructure Working Group	The FFIEC is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the OCC, Federal Reserve, FDIC, National Credit Union Administration, and Consumer Financial Protection Bureau to make recommendations to promote uniformity in the supervision of financial institutions. To encourage the application of uniform examination principles and standards by the state and federal supervisory authorities, the FFIEC established, in accordance with the requirement of the statute, the State Liaison Committee composed of five representatives of state supervisory agencies. In accordance with the Financial Services Regulatory Relief Act of 2006, a representative state regulator was added as a voting member of the FFIEC in October 2006. The FFIEC is responsible for developing uniform reporting systems for federally supervised financial institutions, their holding companies, and the nonfinancial institution subsidiaries of those institutions and holding companies. It conducts schools for examiners employed by the five federal member agencies represented on the FFIEC and makes those schools available to employees of state agencies that supervise financial institutions.
Financial and Banking Information and Infrastructure Committee		In the wake of the attacks on September 11, 2001, the FBIIC was created to focus on three areas: • Improving coordination and communication among financial regulators; • Enhancing the resiliency of the financial sector; and • Promoting public-private partnership. FBIIC members have collaborated since that time to advance the mission of the committee. These efforts are designed to strengthen the security and resiliency of critical infrastructure not only within the financial services sector, but also for the financial institutions regulated or supervised by the FBIIC member organizations.
Basel Committee on Banking Supervision	• Operational Resilience Group • Financial Technology Group	The BCBS is the primary global standard setter for the prudential regulation of banks and provides a forum for regular cooperation on banking supervisory matters. Its 45 members comprise central banks and bank supervisors from 28 jurisdictions.
Financial Stability Board	• Cyber Incident Reporting Working Group	The FSB promotes international financial stability; it does so by coordinating national financial authorities and international standard-setting bodies as they work toward developing strong regulatory, supervisory and other financial sector policies. The FSB fosters a level playing field by encouraging coherent implementation of these policies across sectors and jurisdictions.

Organization	Key Cybersecurity-Related Subgroups	Description
Senior Supervisors Group	• Cybersecurity and Operational Resilience Working Group	The Senior Supervisors Group (SSG) is a forum for senior representatives of supervisory authorities to engage in dialogue on risk management practices, governance, and other issues concerning complex, globally active financial institutions. The group is comprised of senior executives from the bank supervisory authorities of those institutions' home jurisdictions. The SSG leverages the network of relationships in the Group to share information on supervisory approaches and also engages with the financial services industry to better understand new challenges and emerging risks that systemically important institutions face.

Appendix D: Abbreviations

BCBS	Basel Committee on Banking Supervision
CAA	Consolidated Appropriations Act, 2021
CAT	cybersecurity assessment tool
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CPO	Chief Privacy Officer
CRO	Chief Risk Officer
DHS	U.S. Department of Homeland Security
OCC	Office of the Comptroller of the Currency
FBIIC	Financial and Banking Information Infrastructure Committee
FDIC	Federal Deposit Insurance Corporation
FFIEC	Federal Financial Institutions Examination Council
FISMA	Federal Information Security Modernization Act of 2014
FSB	Financial Stability Board
FS-ISAC	Financial Services Information Sharing and Analysis Center
FSSCC	Financial Services Sector Coordinating Council
GAO	Government Accountability Office
IT	information technology
LBS	Large Bank Supervision
MCBS	Midsize and Community Bank Supervision
MRA	matters requiring attention
NIST	National Institute of Standards and Technology
NPR	notice of proposed rulemaking
OIG	Office of the Inspector General
RAS	risk assessment system
SDC	senior deputy comptroller
SyRIS	Systemic Risk Identification Support & Specialty Supervision
URSIT	Uniform Rating System for Information Technology