Office of the Comptroller of the Currency

Cybersecurity and Financial System Resilience Report

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

July 2023

Contents

Preface **1**

Executive Summary **2**

Policies and Procedures to Safeguard Against Cybersecurity Threats **4**
Oversight of OCC-Supervised Banks 4
Cybersecurity-Related Regulations 4
Supervisory Guidance and Resources 5
Examination Manuals 6
Outreach Efforts 7
OCC Internal Security 7

Implementation of Cybersecurity Policies and Procedures **9**
Oversight of OCC-Supervised Banks 9
Staffing and Resources 9
Bank Supervision Activities 10
Interagency Supervision Activities 13
Bank's Efforts to Respond to Cybersecurity and Resilience Concerns 14
Efforts to Respond to Independent Reviews of OCC Supervision 15
Domestic and International Coordination on Cybersecurity 15
OCC Internal Security 17

Current and Emerging Cybersecurity Threats **19**
Oversight of Supervised Institutions 19
Cybersecurity Threat Information Sharing 19
Current and Emerging Cybersecurity Threats 19
OCC Internal Security 21

Appendixes **23**
Appendix A: Cybersecurity Supervisory Guidance and Resources (2015–Present) 23
Appendix B: Key Examination Booklets 25
Appendix C: Examples of Domestic and International Interagency Organizations in Which the OCC Participates 0
Appendix D: Abbreviations 0

Preface

The Consolidated Appropriations Act, 2021,[1] requires the Office of the Comptroller of the Currency (OCC) to issue an annual report to Congress for seven years, beginning in 2021, 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 Consolidated Appropriations Act, 2021, 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 operational resilience and cybersecurity 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, such as
  - the appointment of qualified staff, provision of staff training, use of accountability measures to support staff performance, and 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 U.S Department of the Treasury's inspector general or the independent evaluation described under FISMA.
  - 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. 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 (collectively the "federal banking system").[2] As of September 30, 2022, the federal banking system comprised 1,035 banks operating in the United States. These banks range from small community banks to the largest, most globally active U.S. banks. Of these banks, 775 have less than $1 billion in assets, while 55 have more than $10 billion. In total, the banks within the federal banking system, excluding federal branches and agencies of foreign banks, hold $15.2 trillion of all assets of U.S. commercial banks (64 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-party service providers 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 Board) and the Federal Deposit Insurance Corporation (FDIC).

The OCC views operational resilience and cybersecurity as top issues for the federal banking system and has reiterated this in the OCC's Fiscal Year 2023 Bank Supervision Operating Plan by making them key priorities for supervisory strategies.[5] Cyberattacks continue to compromise security of technology systems, affect operations, and result in breaches of sensitive information across all sectors, including banking. Cyberattacks become more sophisticated and damaging each year. Recent OCC *Semiannual Risk Perspective* reports emphasize the importance of banks continuing to strengthen their risk posture and remaining vigilant of malicious actors' efforts to circumvent cybersecurity controls.[6]

Given continued cyber threats in the financial sector and heightened geopolitical tensions due to Russia's invasion of Ukraine, the OCC continues to place a high priority on interagency and financial sector communications focusing on the importance of monitoring threats and sharing information. The OCC closely coordinates with U.S. Department of the Treasury's Office of Cybersecurity and Critical Infrastructure Protection (OCCIP), financial sector regulators, law enforcement agencies, and the U.S. Department of Homeland Security's (DHS) Cybersecurity and Infrastructure Security Agency (CISA), to monitor cybersecurity risks and potential threats to the U.S. financial system. The OCC also coordinates, as appropriate, with industry partners through the Financial Services Sector Coordinating Council (FSSCC) and Financial Services Information Sharing and Analysis Center (FS-ISAC). When appropriate, the OCC communicates

[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 *2022 Annual Report*.

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

[5] Refer to OCC News Release 2022-124, "OCC Releases Bank Supervision Operating Plan for Fiscal Year 2023."

[6] Refer to the OCC's *Semiannual Risk Perspective*, June 14, 2023.

alerts and other identified risks and threats to supervised financial institutions, often in coordination with interagency partners.

This report discusses actions the OCC is taking to address heightened operational resilience and cybersecurity 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 operational resilience and cybersecurity.
- supervisory processes and banks' efforts to implement and maintain effective cybersecurity and operational resilience risk management practices and controls to safeguard against current and emerging threats.
- internal OCC cybersecurity policies, practices, and controls to safeguard sensitive information and assets that the agency maintains.
- views on operational resilience and cybersecurity 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 contributing to the effective oversight and supervision of the federal banking system in collaboration 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 safe and sound practices, such as those 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 operational resilience and cybersecurity risks in the federal banking system.

Cybersecurity-Related Regulations

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

- **Safety and soundness standards**: The "Interagency Guidelines Establishing Standards for Safety and Soundness Standards," 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 require insured banks to have internal controls and information systems appropriate for the size of the institution and 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 insured banks to have internal audit systems that provide for adequate testing and review of information systems. In addition, the "Guidelines Establishing Heightened Standards for Certain Large Insured National Banks, Insured Federal Savings Associations, and Insured Federal Branches," 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.[8]
- **Safeguarding customer information**: Pursuant to Title V, Subtitle A, of the Gramm–Leach–Bliley Act,[9] the OCC implemented guidelines 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 Standards."

[7] For example, refer to *Comptroller's Handbook* and the *Federal Financial Institutions Examination Council's IT Examination Handbook*.

[8] For purposes of 12 CFR Part 30, appendix D, the term covered bank means any bank: (i) With average total consolidated assets equal to or greater than $50 billion; (ii) with average total consolidated assets less than $50 billion if that bank's parent company controls at least one covered bank; or (iii) with average total consolidated assets less than $50 billion, if the OCC determines that the bank's operations are highly complex or otherwise present a heightened risk as to warrant the application of the Guidelines pursuant to the Reservation of Authority in the Guidelines (Appendix D, I.C).

[9] Refer to 15 USC 6801–6809.

These interagency guidelines require banks to implement an information security program 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 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 illegal activity or a violation of the Bank Secrecy Act.[10] This includes expectations for reporting certain computer crimes.[11]
- **Computer-security incident notification rule**: On November 23, 2021, the OCC, the FDIC, and the Federal Reserve Board published a final rule to establish computer security incident notification requirements for banking organizations and their bank service providers.[12] The rule requires a bank to notify its primary regulator as soon as possible and no later than 36 hours after the bank determines that a computer security incident that rises to the level of a notification incident has occurred.[13] The rule also requires a bank service provider to notify at least one bank-designated point of contact at each affected customer bank as soon as possible when the bank service provider determines it has experienced a computer security incident that has materially disrupted or degraded, or is reasonably likely to materially disrupt or degrade, covered services provided to the bank for at least four hours.

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"[14]
- "Joint Statement on Security in a Cloud Computing Environment"[15]
- "Joint Statement on Heightened Cybersecurity Risk"[16]

[10] Refer to 12 CFR 21.11 and 163.180.

[11] Refer to FinCEN Advisory - FIN-2016-A005, "Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime".

[12] Refer to OCC Bulletin 2021-55, "Computer-Security Incident Notification: Final Rule" and 12 CFR 53.

[13] Refer to OCC Bulletin 2022-8, "Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications."

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

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

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

- "FFIEC Statement on Authentication and Access to Financial Institution Services and Systems"[17]

Many cybersecurity publications and resources have been coordinated through the Federal Financial Institutions Examination Council (FFIEC).[18] 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 IT Examination Handbook,* existing supervisory guidance, and concepts from industry standards, including the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF).

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 publications and resources can be accessed on the FFIEC Cybersecurity Awareness web page. The OCC will continue to review and update existing supervisory approaches to include improvements to the OCC's cybersecurity examination work program.

In addition to OCC and interagency publications and resources, the OCC regularly communicates to banks and service providers regarding other U.S. government agency guidance and relevant alerts. Examples include alerts on critical vulnerabilities being actively targeted by cyber threat actors or increasing geopolitical tensions, such as CISA's Alert AA22-011a, "Understanding and Mitigating Russian State-Sponsored Cyber Threats to U.S. Critical Infrastructure," and information on CISA's Shields Up program.

Appendix A of this report provides a list of key cybersecurity-related supervisory guidance statements and other resources published by the OCC and its regulatory partners from 2014 to 2023.

Examination Manuals

The OCC oversees the federal banking system by implementing and enforcing federal banking laws 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

[17] Refer to OCC Bulletin 2021-36, "Information Security: FFIEC Statement on Authentication and Access to Financial Institution Services and Systems."

[18] The FFIEC, established in 1979, comprises the OCC, FDIC, Federal Reserve Board, National Credit Union Administration, Consumer Financial Protection Bureau, and the State Liaison Committee.

nationwide.[19] 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.*[20]

The OCC uses the FFIEC's Uniform Rating System for Information Technology (URSIT) to assess and rate 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.[21]

For detailed IT information and work programs, OCC examiners use the *Comptroller's Handbook* and the *FFIEC IT Examination Handbook*. The *FFIEC IT Examination Handbook* is a series of booklets addressing IT-related supervision topics. The booklets include examination work programs. Aspects of cybersecurity are in various booklets such as "Management," "Information Security," "Business Continuity Management," and "Architecture, Infrastructure, and Operations."[22]

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.

Outreach Efforts

The OCC regularly engages in outreach efforts to engage with banks and other stakeholders to communicate operational resilience and cybersecurity 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, chief information officers, chief technology officers, and chief information security officers, to better structure content, including topics related to operational resilience and cybersecurity. Additionally, OCC subject matter experts speak at industry-sponsored forums on cybersecurity, operational resilience, and third-party risk management.

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 supervisory 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 (OMB), CISA, and NIST.

[19] Refer to the OCC's *2022 Annual Report*.

[20] For example, refer to "Bank Supervision Process" booklet of the *Comptroller's Handbook.*

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

[22] Refer to the FFIEC IT Examination Handbook InfoBase.

- 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; and
- information security awareness and privacy training.

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 tools and services employing industry and federal sources; and
- operation of a mature enterprise logging infrastructure to support continuous monitoring of all network traffic and event correlation for the discovery of anomalous cyber activity across the network and its end hosts. This reflects direction as outlined in OMB M-21-31, "Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents," in accordance with Executive Order 14028, "Improving the Nation's Cybersecurity."

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 incident. The OCC published its supervisory priorities in its Fiscal Year 2023 Bank Supervision Operating Plan to provide the foundation for policy initiatives and supervisory strategies as applied to individual national banks, federal savings associations, federal branches, federal agencies, and technology service providers, listing operational resilience and cybersecurity as a top priority.[23]

Oversight of OCC-Supervised Banks

Staffing and Resources

As of the September 30, 2022, the OCC had approximately 2,262 bank examiners.[24] 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 and technology, such as ransomware and distributed ledger technology. All safety and soundness examiners receive sufficient training to conduct IT and cybersecurity examinations at noncomplex community banks.

In addition to safety and soundness 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 (ISC)² Certified Information Systems Security Professional.[25] To gain further expertise on IT and cybersecurity topics, IT specialist examiners regularly attend industry conferences to learn of emerging trends and risks and to take advanced external training.

Examiners are generally assigned to Large Bank Supervision or Midsize and Community Bank Supervision. Large Bank Supervision oversees banks that have between $50 billion and $3 trillion in assets. In Midsize and Community Bank Supervision, examiners can be assigned to Midsize Bank Supervision or one of the OCC's geographic regions responsible for community bank supervision. Midsize Bank Supervision generally oversees banks with between $10 billion and $75 billion in assets, and the geographic regions supervise community banks with less than $10 billion in assets.

In addition to examiners in Large Bank Supervision and Midsize and Community Bank Supervision, the OCC has additional supervision and subject matter expert resources that support cybersecurity oversight and supervision, including:

[23] Refer to OCC News Release 2022-124, "OCC Releases Bank Supervision Operating Plan for Fiscal Year 2023."

[24] Refer to the OCC's *2022 Annual Report*.

[25] Refer to ISACA's CISA certification page and (ISC)²'s CISSP certification page.

- The Systemic Risk Identification & Support (SyRIS) division identifies, evaluates, and collaborate with intra- and interagency counterparts to holistically assess and address risks that impact the OCC's mission as it relates to supervision, provides subject matter expertise across all risk disciplines, assists in resource prioritization, and provides direct supervision of services provided by significant service providers.
- Bank Supervision Policy (BSP) maintains two policy units that focus on operational resilience and cybersecurity risks:[26]
  - The Bank Information Technology (BIT) Policy unit develops and maintains supervisory guidance, resources, examination manuals, and supervisory tools that help examiners conduct cybersecurity supervision, such as the *FFIEC IT Examination Handbook* and related work programs.
  - The Critical Infrastructure Policy unit identifies and assesses systemic operational risks that could degrade or interrupt the federal banking system and lead to national economic concerns. The unit also supports the coordination of internal responses and information sharing during critical infrastructure events, such as cybersecurity incidents.
- The Office of Financial Technology, within BSP, is the OCC's 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 can include coordination on issues related to operational resilience and cybersecurity for new or innovative products, services, and technologies.

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.[27] 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 authority to examine a bank as frequently as the OCC deems appropriate.[28] As part of every

[26] BSP 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.

[27] 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.*

[28] 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.

supervisory cycle, the OCC conducts an IT assessment for each bank that includes an examination of cybersecurity risk management and controls.

The supervisory strategy is the OCC's detailed supervisory plan for each bank, outlining 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.[29] The *FFIEC IT Examination Handbook* has detailed work programs that supplement the core assessment.
- **Risk assessment system:** The OCC's risk assessment system is a concise method of communicating and documenting conclusions on eight risk categories: credit, interest rate, liquidity, price, operational, compliance, strategic, and reputation. Examiners draw conclusions on 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 risk assessment system conclusions for relevant risk categories, such as operational, compliance, strategic, and reputation.[30]
- **Cybersecurity examination work programs**: The OCC continues to review and update supervisory approaches.
    - In response to an increase in the number of disruptive and destructive cyberattacks involving ransomware, the OCC incorporated specific supplemental examination procedures to the agency's planned cybersecurity supervisory activities as part of the fiscal year 2022 supervision cycle. These procedures focused on an assessment of key risk management and control elements for a bank's preparedness against disruptive and destructive ransomware attacks by providing insight into the adequacy of banks' preventative controls, data backup processes, and incident response program.
    - In fiscal year 2023 the OCC updated its approach to cybersecurity assessment as part of the agency's supervision of banks. The Cybersecurity Supervision Work Program (CSW)[31] is a component of the OCC's risk-based BIT supervision process. The CSW provides high-level examination objectives and procedures

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

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

[31] Refer to the Cybersecurity Supervision Work Program Overview | OCC

that are aligned with existing supervisory guidance and the NIST-CSF.[32] Recognizing that OCC-supervised banks use different frameworks to manage their cybersecurity programs, the CSW cross-references OCC examination procedures to the NIST-CSF, *FFIEC IT Examination Handbook*, and other common industry cybersecurity frameworks. The CSW does not introduce any new supervisory expectations. The OCC continues to encourage but does not require banks' use of a standardized approach to assess cybersecurity preparedness.[33]

- **Ongoing supervision:** Ongoing supervision is the OCC's process for assessing risks and reviewing core knowledge about a bank. Ongoing supervision conclusions can result in changes to the OCC's supervisory strategy, regulatory ratings, or risk assessment system conclusions for a bank.
- **Other resources**: Examiners use cybersecurity concepts that are communicated in or through the supervisory publications, such as the *FFIEC IT Examination Handbook.* Other resources include:
  - the NIST-CSF.
  - the Center for Internet Security Critical Security Controls.[34]
  - the Cyber Risk Institute's Financial Sector Cybersecurity Profile.[35]
  - MITRE ATT&CK.[36]
  - alerts and guidance issued from such organizations as CISA and law enforcement.
- **Communicating examination findings**: As part of the supervision process, the OCC is committed to ongoing, effective communication with supervised banks, such as 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,[37] 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

[32] Refer to the NIST-CSF.

[33] Refer to "FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness," August 28, 2019.

[34] Refer to Center for Internet Security's Critical Security Controls.

[35] Refer to the Cyber Risk Institute's Profile.

[36] Refer to the MITRE ATT&CK page.

[37] A deficient practice is a practice, or lack of practice, 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.

may serve as the basis for an enforcement action. Formal enforcement actions are public and may be 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.[38]

Interagency Supervision Activities

The OCC actively coordinates with the FDIC and Federal Reserve Board on operational resilience and cybersecurity 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, increase efficiencies in the use of cybersecurity supervision subject matter experts across the agencies, and provide more effective supervision of highly complex organizations.

Another example of interagency coordination is the examination of services performed by significant third parties for supervised banks. Service providers can pose a significant risk to their clients and 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 Board, and when applicable, with the participation of state banking regulators. Key aspects of the service provider examination program include:

- 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 at service providers follow interagency guidelines and use the *FFIEC IT Examination Handbook* and other applicable guidance.[39]
- Annual strategies are developed for service provider examination activities. The strategies define supervisory goals for a specific service provider based on its risk profile of services provided, including cybersecurity-related activities and emerging risks across the industry.
- The OCC, FDIC, and Federal Reserve Board have implemented a consistent framework for cybersecurity assessments for service providers, based on the *FFIEC IT Examination Handbook*.

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

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

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

Bank's Efforts to Respond to Operational Resilience and Cybersecurity 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 important 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 key risk. The Spring 2023 report featured cybersecurity as an elevated risk as cyberattacks continue to evolve,[40] become more sophisticated, and inflict damage on the U.S. economy. Increasing geopolitical tensions have also elevated cyber risks and highlight the importance of heightened threat monitoring and safeguarding against disruptive attacks targeting the financial sector. Cyber actors continue to exploit publicly known and dated software vulnerabilities and weak authentication against broad target sets, including banks and financial service providers. Ransomware attacks in financial services continue to increase. These attacks use phishing emails that target employees with the goal of compromising credentials to gain access to networks. After access is gained, the actors conduct ransomware and other extortion campaigns. Distributed denial of service attacks also continue to take place.

To mitigate against cyber risks, it is important for banks to maintain heightened threat and vulnerability monitoring processes and implement more stringent security measures, including the use of multifactor authentication, hardening of systems configurations, and timely patch management. Banks also should consider how to effectively implement, regularly test, and isolate system backups from network connections to provide operational resilience.

Prolonged use of older or legacy systems can also introduce security vulnerabilities, create system maintenance challenges, and cause issues that reduce the resilience of operations. While OCC-supervised banks continue to invest significant resources in maintaining and updating existing technology architecture, some banks encounter challenges keeping up with technological advances while maintaining legacy infrastructure. Decisions to postpone system updates or delay technology architecture upgrades can create unwarranted risks to an organization. OCC supervision has focused on technology resilience and has identified supervisory concerns related to end-of-life, patch management, and system and data architecture. Banks should align technology architecture planning with their cybersecurity programs to ensure that systems are appropriately maintaining adequate safeguards against cyber threats and can maintain resilient operations.

The risk to supply chain management operations continues to increase and evolve as attacks target vulnerabilities in software systems commonly used by large numbers of organizations. Threat actors are increasingly exploiting vulnerabilities in IT systems and third-party software to conduct malicious cyber activities while negotiating ransom payments. These attacks demonstrate the need for banks to assess the risks arising from their third parties and develop a comprehensive approach to operational resilience and supply chain risk.

[40] Refer to the OCC's *Semiannual Risk Perspective*, June 14, 2023.

Recent *Semiannual Risk Perspective* reports continue to highlight the key role that banks' third-party relationships can have on operational resilience and cybersecurity. Effective risk management for critical third-party relationships is important for safe and sound operations. The OCC, FDIC, and Federal Reserve Board issued interagency guidance on risk management for third-party relationships on June 6, 2023.[41] This update of existing third-party risk management guidance includes key considerations for operational resilience and cybersecurity when engaging third parties.

Efforts to Respond to Independent Reviews of OCC Supervision

The OCC is subject to oversight by the Treasury Department's Office of the Inspector General (OIG) and the U.S. 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.

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. Through the FFIEC's Task Force on Supervision, groups such as the Cybersecurity and Critical Infrastructure Subcommittee and the Information Technology Subcommittee have developed and published a wide range of documents and resources for assessing cybersecurity risks.

The OCC actively coordinates with the Treasury Department's OCCIP and the broader financial sector regulatory agencies by participating on the Financial and Banking Information Infrastructure Committee (FBIIC).[42] 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 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 incidents and other significant events that affect the financial sector. In 2022, the OCC collaborated with FBIIC members to identify cloud service use in the financial sector and security and resilience risks and challenges associated with the increasing trend of financial sector firms adopting cloud service technology.[43]

[41] Refer to OCC Bulletin 2023-17, "Third-Party Relationships: Interagency Guidance on Third-Party Relationships: Risk Management."

[42] Refer to the FBIIC.

[43] Refer to "New Treasury Report Assesses Opportunities, Challenges Facing Financial Sector Cloud-Based Technology Adoption," February 8, 2023.

In addition to coordinating with domestic regulatory counterparts, the OCC engages with industry groups, as appropriate. The OCC engages with the FSSCC, through the FBIIC, to coordinate on 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*.

The OCC partners with federal agencies to coordinate cyber incident reporting efforts. In March 2022 President Biden signed the Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) into law.[44] CIRCIA requires covered entities to report covered cyber incidents and ransomware payments to CISA. The OCC participates on the intergovernmental Cyber Incident Reporting Council (CIRC), established by CIRCIA, tasked with coordinating, deconflicting, and harmonizing federal incident reporting requirements. DHS, in consultation with CIRC members, is required to provide Congress a report identifying duplicative reporting requirements, challenges to harmonization, actions the CISA Director intends to take to facilitate harmonization, and any proposed legislative changes to address duplicative reporting. The ongoing work of the CIRC should also complement and inform CISA's implementation efforts under CIRCIA.

The OCC is actively participating in the Cybersecurity Forum for Independent and Executive Branch Regulators. The forum's purpose is to increase the overall effectiveness and consistency of regulatory agency cybersecurity efforts pertaining to U.S. critical infrastructure. Additionally, the forum seeks to identify and explore opportunities to promote a united effort across participating agencies and to use and deconflict cross-sector regulatory authorities' approaches to strengthen the nation's cybersecurity posture. The forum meets monthly to discuss broad government cybersecurity goals outlined in Executive Order 14028 and coordinate implementation of CIRCIA.

The OCC coordinates regularly with the FS-ISAC for threat and vulnerability monitoring and resilience efforts. FFIEC members issued a statement encouraging financial institutions to join and engage with FS-ISAC to increase participation and coordination.[45] When appropriate, the OCC engages with law enforcement and other government agencies regarding threat information or specific issues affecting financial institutions.

Another example of OCC coordination efforts is the Hamilton series of 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 and private sector coordination. A key outcome resulting from the exercises is Sheltered Harbor, a voluntary industry initiative for data vaulting to safeguard critical data in the event of a destructive malware attack.[46] The OCC issued an interagency statement noting that

[44] Refer to Cyber Incident Reporting For Critical Infrastructure Act of 2022 (cisa.gov)

[45] Refer to FFIEC press release, "FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center." November 3, 2014.

[46] Refer to "Sheltered Harbor's Mission."

institutions should consider whether their backup and restoration practices are consistent with industry standards and frameworks, including Sheltered Harbor.[47]

The OCC regularly engages internationally on operational resilience and cybersecurity -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. Examples of publications from these groups are BCBS's *Principles for Operational Resilience* (March 31, 2021); FSB's *Recommendations to Achieve Greater Convergence in Cyber Incident Reporting: Final Report* (April 13, 2023); 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 operational resilience and cybersecurity related matters.

OCC Internal Security

The OCC Chief Information Officer (CIO) designates the OCC Chief Information Security and Chief Privacy Officer (CISO) to fulfill the CIO's responsibilities under FISMA. OCC hiring procedures for the CISO are designed to ensure that this individual has the requisite professional qualifications and singular mission focus to conduct 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 security and cybersecurity risks. The key program areas within CSO are 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 skill development along with CISO priorities in areas of interest, such as zero trust architecture and 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: 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, with

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

ongoing tracking and reporting available to management to encourage individual accountability for protecting OCC information.

Senior appointed leaders at the OCC are responsible for signing and attesting that the agency has met FISMA's annual reporting requirement. The Comptroller, OCC Senior Deputy comptrollers, and the OCC Chief Risk Officer (CRO) receive monthly cybersecurity/privacy briefings and ad hoc briefs from the CISO. Senior deputy comptrollers serve on senior executive subcommittees focusing on technology investment and enterprise risk management.

Adequate resources and technologies for implementing the OCC's Information Security and Cyber Protection program are allocated using a risk-based approach that integrates the CIO's work intake and planning processes with agency budget activities. The CIO collaborates with the OCC senior executive subcommittee on technology investment to prioritize capital investment projects that address the most significant technology risks to the agency, including cybersecurity risks. The CIO reports cybersecurity status and major investments to this subcommittee. 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 2022 FISMA audit and has maintained a "Managing Risk" rating for its performance on quarterly CIO FISMA metrics. The OCC received important assurance in March 2023 from an independent assessment by a leading cybersecurity service confirming no instances of any advanced persistent threat in the agency's IT network environment.

The CSO manages a plan of actions and milestones process that ensures tasks and action items are developed in response to any findings or weaknesses in security and privacy controls identified through regular internal assessments or routine operational security activities. This process also 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 and OMB in response to cybersecurity directives and tasks. The OCC ensures that all CISA and OMB reporting is shared with the Treasury Department to facilitate cross-departmental information sharing and collaboration on cyber threats and vulnerabilities. Formal and informal collaboration, consultation, and benchmarking on key cybersecurity issues are conducted with other regulatory agencies and FFIEC member agencies.

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 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, 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 several mechanisms to identify and measure current and emerging risks to the banking sector. One of the key groups focused on this analysis is the OCC's National Risk Committee. Members include senior agency officials who supervise banks of all sizes and develop bank supervisory policy. The 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. The OCC has been most focused on the following current and emerging operational resilience and cybersecurity threats to the banking sector.

- **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 cyberattack. The financial sector has also seen an increase in ransomware developers adopting a ransomware-as-a-service (RaaS) model, in which the developers of a ransomware strain allow other cyber criminals, known as affiliates, to use an administrator's malware to conduct attacks in exchange for a small, fixed cut of ransom proceeds.

- **Distributed denial of service (DDoS):** DDoS attacks come in a variety of shapes and sizes and require different mitigations to counter the wide variety of attacks. The FFIEC issued a joint statement in 2014 encouraging banks and their service providers to address DDoS readiness as part of ongoing information security and incident response plans.[48]
- **Account takeover:** Cyber criminals have used several 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 service providers. Recent high-profile incidents demonstrate the importance of banks assessing the risks emanating from their suppliers and third parties and developing a comprehensive cooperative approach to operational resilience.
- **Geopolitical threats:** Increased geopolitical tensions have further heightened the risk of the Russian government exploring options for potential cyberattacks in response to the unprecedented economic sanctions imposed in response to Russia's invasion of Ukraine. These tensions highlight the importance of heightened threat monitoring, greater public-private sector information sharing, and safeguarding against disruptive attacks targeting the financial sector. The OCC has worked with other agencies to develop and distribute information and resources on heightened risk from cybersecurity threats and mitigations. The OCC and other agencies continue to highlight CISA's efforts to promote awareness and mitigation of current cybersecurity threats on CISA's Shields Up web page.
- **Post-quantum cryptography:** Quantum computing is an emerging technology with security implications that could make current encryption technology ineffective. While broad implementation of quantum computing is unlikely be available in the near term, banks and service providers should be aware of the risk implications and should consider how to effectively monitor developments in quantum computing as they manage future infrastructure investments.
- **Intersection of crypto-assets and cyber risks:** The crypto-asset sector has experienced significant volatility and turmoil. The *Semiannual Risk Perspective for Spring 2023* highlights risks related to crypto-asset activities, including the frequency of hacks and

[48] Refer to OCC Bulletin 2014-14, "Distributed Denial-of-Service Cyber Attacks, Risk Mitigation, and Additional Resources: Joint Statement."

outages and the high degree of fraud and scams within the crypto industry.[49] On January 3, 2023, the OCC, FDIC, and Federal Reserve Board issued a joint statement on crypto-asset risks to banking organizations that may include vulnerabilities related to cyberattacks, outages, lost or trapped assets, and illicit finance, particularly with open, public, and decentralized networks, or similar systems. The OCC continues to maintain a careful, cautious approach to bank current and proposed crypto-asset activities.[50]

Current and emerging operational resilience and cybersecurity threats are communicated to OCC-supervised banks, service providers, and other stakeholders through a number of channels, including the *Semiannual Risk Perspective*.[51] 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 operational resilience and cybersecurity as key risks to the industry.

OCC resources monitor longer-term technology developments that may affect operational resilience and cybersecurity in the future. These emerging developments and technological advances can strengthen security or create new cybersecurity risks as malicious actors seek to exploit them. OCC subject matter experts, including Office of Financial Technology staff, monitor these longer-term developments and engage with stakeholders to assess their potential impact on the financial sector. An example of these efforts is the interagency request for information on financial institutions' use of artificial intelligence, including machine learning.[52] This request included questions on how the use of artificial intelligence technologies may affect cybersecurity.

OCC Internal Security

CSO's threat intelligence team continually monitors industry and federal threat intelligence sources, including the Treasury Department, CISA, and FS-ISAC, to identify emerging threats to the OCC. The CISO delivers monthly reports to the Comptroller and Executive Committee members, including the CRO, on current cybersecurity threats to the OCC identified by CSO's 24/7/365 Cyber Defense 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, denial of service, and unauthorized access attempts by malicious actors, which include nation-state actors that pose risk to the confidentiality, integrity, and availability of OCC information.

[49] Refer to the OCC's *Semiannual Risk Perspective*, June 14, 2023.

[50] Refer to OCC Bulletin 2023-1, "Crypto-Assets: Joint Statement on Crypto-Asset Risks to Banking Organization."

[51] Refer to the OCC's *Semiannual Risk Perspective*, June 14, 2023.

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

Appendices

Appendix A: Cybersecurity Supervisory Guidance and Resources (2014–Present)

Organization	Date	Document type	Title	Description
OCC	June 26, 2023	Bulletin	OCC Bulletin 2023-22 "Cybersecurity: Cybersecurity Supervision Work Program"	Highlights the CSW for use by OCC examiners.
OCC, FDIC, Federal Reserve Board, Consumer Financial Protection Bureau, National Credit Union Administration, and State Financial Regulators (SFR)	June 6, 2023	Joint Statement	Interagency Message on Critical Vulnerability Affecting MOVEit Transfer	Highlights a critical vulnerability, tracked as CVE-2023-34362, impacting the MOVEit Transfer web application.
OCC, FDIC, Federal Reserve Board	June 6, 2023	Guidance for comment	OCC Bulletin 2023-17 "Third-Party Relationships: Interagency Guidance on Third-Party Relationships: Risk Management"	Replaces the OCC's existing third-party risk management guidance from 2013, the interagency guidance replaces each agency's existing guidance on this topic, and is directed to all banking organizations supervised by the agencies.
OCC, FDIC, Federal Reserve Board	January 3, 2023	Joint Statement	OCC Bulletin 2023-1, "Crypto-Assets: Joint Statement on Crypto-Asset Risks to Banking Organizations"	Highlights key risks to banks associated with crypto-assets and crypto-asset sector participants.
FFIEC	October 6, 2022	Resource	OCC Bulletin 2022-22, "Cybersecurity: 2022 Cybersecurity Resource Guide for Financial Institutions"	Provides a list of voluntary programs and actionable initiatives that are designed for or available to help financial institutions meet their security control objectives and prepare to respond to cyber incidents.
OCC	March 29, 2022	Bulletin	OCC Bulletin 2022-08, "Information Technology: OCC Points of Contact for Banks' Computer-Security Incident Notifications"	Provides OCC points of contact that banking organizations may use to satisfy the notification requirement in 12 CFR 53.
FFIEC	August 11, 2021	Guidance	OCC Bulletin 2021-36, "Information Security: FFIEC Statement on Authentication and Access to Financial	Describes significant risks associated with the cybersecurity threat landscape and the importance of banks effectively authenticating users and customers. The guidance recognizes that

Organization	Date	Document type	Title	Description
			Institution Services and Systems"	authentication considerations extend beyond customers to include employees, third parties, and system-to-system communications.
OCC, FDIC, Federal Reserve Board	October 30, 2020	Sound practices	OCC Bulletin 2020-94, "Operational Risk: Sound Practices to Strengthen Operational Resilience"	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 widespread disruption.
FFIEC	April 30, 2020	Joint statement	OCC Bulletin 2020-46, "Cybersecurity: Joint Statement on Security in a Cloud Computing Environment"	Addresses use of cloud computing services and security risk management principles in the financial services sector.
OCC, FDIC	January 16, 2020	Joint statement	OCC Bulletin 2020-5, "Cybersecurity: Joint Statement on Heightened Cybersecurity Risk"	Reiterates sound cybersecurity risk management principles.
FFIEC	November 5, 2018	Joint statement	OCC Bulletin 2018-40, "Cybersecurity: Cyber-Related Sanctions"	Alerts financial institutions to actions taken by the Treasury Department's Office of Foreign Assets Control under its 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	April 10, 2018	Joint statement	OCC Bulletin 2018-8, "Cyber Insurance: FFIEC Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs"	Provides awareness of the potential role of cyber insurance in financial institutions' risk management programs.
FFIEC	May 2017	Resource	Cybersecurity Assessment Tool	Provides a repeatable, measurable process for financial institutions to measure their cybersecurity preparedness over time. The CAT incorporates cybersecurity-related principles from the *FFIEC IT 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	OCC Bulletin 2016-18, "Cybersecurity of Interbank Messaging and Wholesale Payment Networks: FFIEC Statement"	Reminds financial institutions of the importance of actively managing the risks associated with interbank messaging and wholesale payment networks.

Organization	Date	Document type	Title	Description
FFIEC	November 2015	Joint statement	"Cyber Attacks Involving Extortion"	Notifies financial institutions of the increasing frequency and severity of cyberattacks involving extortion.
FFIEC	March 30, 2015	Joint statement	OCC Bulletin 2-15-20, "Cybersecurity: Destructive Malware Joint Statement"	Notifies financial institutions of the increasing threat of cyberattacks involving destructive malware.
FFIEC	March 30, 2015	Joint statement	OCC Bulletin 2015-29, "Cybersecurity: Cyber Attacks Compromising Credentials Joint Statement"	Addresses growing trend of cyberattacks to obtain online credentials for theft, fraud, or business disruption and to recommend risk mitigation techniques.
FFIEC	November 3, 2014	Joint statement	OCC Bulletin 2014-53, "Cybersecurity: Cybersecurity Assessment General Observations and Statement"	Recommends 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 focus on: • 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 IT Examination Handbook*	The *FFIEC IT Examination Handbook* comprises multiple booklets addressing: • Architecture, Infrastructure, and Operations • Audit • Business Continuity Management • Development and Acquisition • 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 in Which the OCC Participates

Organization	Key Cybersecurity-Related Subgroups	Description
BCBS	• Operational Resilience Group • Financial Technology Group • Supervision Cooperation 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.
FBIIC		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. • Promoting public-private partnership. FBIIC members have collaborated since then to advance the committee's mission. 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.
FFIEC	• Task Force on Supervision • Information Technology Subcommittee • Cybersecurity and Critical Infrastructure Subcommittee	The FFIEC, established on March 10, 1979, pursuant to title X of the Financial Institutions Regulatory and Interest Rate Control Act of 1978 (FIRA), Public Law 95-630. In 1989, title XI of the Financial Institutions Reform, Recovery and Enforcement Act of 1989 (FIRREA), is a formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions by the OCC, FDIC, Federal Reserve Board, National Credit Union Administration, and Consumer Financial Protection Bureau and 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.
FSB	• Cyber Incident Reporting Working Group	The FSB promotes international financial stability 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 (SSG)	• Cybersecurity and Operational Resilience Working Group	The 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 composed of senior executives from the bank supervisory authorities of those institutions' home jurisdictions. The SSG uses the network to share information on supervisory approaches and 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
BSP	Bank Supervision Policy
CAT	Cybersecurity Assessment Tool
CIO	Chief Information Officer
CIRC	Cyber Incident Reporting Council
CIRCIA	Cyber Incident Reporting for Critical Infrastructure Act of 2022
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security and Chief Privacy Officer
CRO	Chief Risk Officer
CSF	Cybersecurity Framework
CSO	Cyber Security Office
CSW	Cybersecurity Supervision Work Program
DHS	Department of Homeland Security
DDoS	Distributed Denial of Service
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	U.S. Government Accountability Office
IT	Information technology
MRA	Matters requiring attention
NIST	National Institute of Standards and Technology
OCC	Office of the Comptroller of the Currency
OCCIP	Office of Cybersecurity and Critical Infrastructure Protection
OIG	Office of the Inspector General
OMB	Office of Management and Budget
SyRIS	Systemic Risk Identification & Support
URSIT	Uniform Rating System for Information Technology