NCUA
National Credit Union Administration

Report to the Committee on Financial Services of the House of Representatives and to the Committee on Banking, Housing, and Urban Affairs of the Senate

on

Cybersecurity and Credit Union System Resilience

June 26, 2023

[This page intentionally left blank]

Cybersecurity & Credit Union Resilience Report • June 2023
Table of Contents

Introduction

Created by the U.S. Congress in 1970, the National Credit Union Administration (NCUA) is an independent federal agency that insures deposits at federally insured credit unions, protects the members who own credit unions, charters and regulates federal credit unions, and promotes widespread financial education and consumer financial protection. Backed by the full faith and credit of the United States, the National Credit Union Share Insurance Fund (NCUSIF) provides up to $250,000 of federal share insurance to more than 136.6 million members in all federal credit unions and most state-chartered credit unions. The NCUA is responsible for the federal regulation and supervision of 4,712 federally insured credit unions with more than $2.2 trillion in assets across all states and U.S. territories as of March 31, 2023.

The NCUA also plays a role in maintaining the nation's financial stability as a member of the Federal Financial Institutions Examination Council (FFIEC) and as a member of the Financial and Banking Information Infrastructure Committee (FBIIC). In addition, the NCUA's Chairman is a voting member of the Financial Stability Oversight Council (FSOC), an interagency body tasked with identifying and responding to emerging risks and threats to the financial system.

Cyberattacks and cybersecurity exposures pose significant risks to the financial system. Because the credit union industry and the broader financial system are vulnerable, cybersecurity is one of the NCUA's top supervisory priorities, and cyberattacks are a top-tier risk under the agency's enterprise risk management program. The NCUA continues to enhance the cybersecurity resilience of credit unions through ongoing improvements to its examination program and by providing credit unions with guidance, information, and resources. Further, the NCUA continuously seeks to improve the security of its own systems and data.

However, significant risks and challenges remain due to the NCUA's lack of authority over third-party vendors that provide services to federally insured credit unions. Given cyber-related incidents affecting credit unions and credit union members often occur at or through third-party vendors, this growing regulatory blind spot has the potential to trigger cascading consequences throughout the credit union industry and the financial services sector that may result in significant losses to the NCUSIF. For this reason, one of the agency's top requests of Congress is to restore the authority, which sunset in 2001, enabling the NCUA to examine third-party vendors. The Financial Stability Oversight Council, the Government Accountability Office, and the NCUA Office of the Inspector General have all called on Congress to close this growing regulatory blindspot.

Recent geopolitical tensions have increased the risks to a credit union's information technology (IT) infrastructure. Many credit unions protect themselves through robust controls to safeguard

against fraud, financial crimes, or operational errors. Prudent credit unions establish a comprehensive operational resilience framework commensurate with the size, scope, and complexity of operations and the products and services offered. Operational resilience depends on ongoing monitoring and adjusting of internal controls, risk management practices, and risk mitigation strategies to adapt to the increasingly complex technology infrastructure and cybersecurity landscape. Credit unions that thrive deliver member services through technology and adopt financial innovation while averting potentially catastrophic cyber risks.

This report provides an explanation of measures taken to strengthen cybersecurity within credit unions and the NCUA, as required by the Consolidated Appropriations Act, 2021.[1] The report outlines policies and procedures to address cybersecurity risks, activities to ensure effective implementation, and any current or emerging threats.

Policies and Procedures

Information Security and Cybersecurity Regulation

The NCUA has broad authority to regulate federal credit unions and all federally insured credit unions through Titles I and II of the Federal Credit Union Act, respectively. Additionally, the NCUA derives authority and direction to regulate credit unions from other applicable laws.

In particular, the Gramm-Leach-Bliley Act requires the NCUA Board to establish appropriate standards for federally insured credit unions relating to administrative, technical, and physical safeguards for member records and information. These safeguards are intended to ensure the security and confidentiality of member records and information; protect against anticipated threats or hazards to the security or integrity of such records; and protect against unauthorized access to or use of such records or information, which could result in substantial harm or inconvenience to any member.

In implementing the Gramm-Leach-Bliley Act requirements, the NCUA issued 12 C.F.R. part 748, Appendix A, Guidelines for Safeguarding Member Information. This guidance governs what federally insured credit unions should do to develop an information security program and contains provisions for credit unions to notify the NCUA of certain information security incidents.

In February 2023, the NCUA Board unanimously approved a final rule that requires insured credit unions to notify the NCUA as soon as possible, within 72 hours, after a credit union

[1] Pub. L. No. 116–260, 134 Stat. 2173 (Dec. 27, 2020)

reasonably believes that a reportable cyber incident has occurred. Under this rule, federally insured credit unions are required to report a cyber incident that leads to a substantial loss of confidentiality, integrity, or availability of a network or member information systems as a result of the unauthorized access to or exposure of sensitive data, disruption of vital member services, or that has a serious impact on the safety and resiliency of operational systems and processes.

Additionally, cyberattacks that disrupt a credit union's business operations, vital member services, or a member information system must be reported to the NCUA within 72 hours of a credit union's reasonable belief that it has experienced a cyberattack. This rule is effective September 1, 2023.

Information Security Examination Program

The NCUA uses a risk-based approach to examining and supervising credit unions. The risk-based approach addresses the following seven primary areas of risk:

- Credit risk;
- Interest rate risk;
- Liquidity risk;
- Transaction risk;
- Compliance risk;
- Strategic risk; and
- Reputation risk.

The NCUA examines all federally insured credit unions periodically.[2] At each examination the NCUA performs an IT review, including reviewing components of information security and cybersecurity, to verify compliance with applicable laws and regulations and maintain safety and soundness. The NCUA uses a risk-focused approach to examine credit unions' IT, which provides examiners the flexibility to focus on areas of current or potential material risk relevant to each credit union's unique business model.

The objectives of the IT examination procedures include:

[2] The NCUA's examination frequency for federal credit unions is based on risk but generally may not extend more than 20 months from the previous examination. Federally insured, state-chartered credit unions are primarily examined by the applicable state regulator, with participation from the NCUA based on risk, but no less than every 60 months.

- Evaluating management's ability to recognize, assess, monitor, and manage information systems and technology-related risks;
- Assessing whether the credit union has sufficient expertise to adequately plan, direct, and manage IT operations;
- Determining whether the board of directors is informed of IT-related risks and has adopted and implemented adequate IT-related policies and procedures; and
- Evaluating the adequacy of internal IT controls and oversight to safeguard member information.

The NCUA began using its new Information Security Examination (ISE) procedures in early 2023. The new ISE procedures were designed to better enable examiners to tailor the examination based on asset size and complexity, standardize the examination of a credit union's information security and cybersecurity program, and enhance the identification of control deficiencies and trends at the industry level. The new ISE procedures also provide examiners and credit unions with a well-structured examination workflow.

The ISE procedures are focused on NCUA regulations parts 748 and 749 and align closely with the voluntary Automated Cybersecurity Evaluation Toolbox (ACET) maturity assessment. ISE also references guidance from the NCUA and the FFIEC, as well as other industry accepted best practices and security frameworks from the National Institute of Standards & Technology (NIST), the Center for Internet Security, and the Cybersecurity and Infrastructure Security Agency.

There are three types of exam-level statements making up the ISE:

- **Small Credit Union Examination Program (SCUEP) statements**: Tailored for credit unions of asset sizes of $50 million and below.
- **Core statements**: Tailored for credit unions of asset sizes greater than $50 million.
- **Core+ statements**: Containing optional examination elements specialists may reference based upon risk.

The NCUA's information security examination program incorporates the criteria below.

- **Information Security Examination**: The NCUA is leveraging lessons learned from IT tools the agency has used in the past as well as industry standards to perform enhanced IT and security examinations and verify compliance with applicable laws, rules, and regulations.

- **Automated Cybersecurity Examination Tool (ACET) Maturity Assessment**: The ACET maturity assessment allows credit unions to determine the maturity of their information security programs. The tool incorporates appropriate cybersecurity standards and practices established for financial institutions. It also maps each of its declarative statements to best practices found in the FFIEC IT Examination Handbook, regulatory guidance, and leading industry standards like the NIST Cybersecurity Framework.
- **Examiner's Guide**: The Examiner's Guide provides a framework for consistent application of staff judgment with respect to conclusions about a credit union's financial and operational condition and related risk ratings. It also provides a consistent approach for evaluating the adequacy of a credit union's relevant risk management processes. The Examiner's Guide and other related examiner guidance, manuals, and training materials provide examiners with information and direction with respect to the NCUA's IT examination policies and procedures.
- **National Supervision Policy Manual (NSPM)**: The NSPM establishes national policies, procedures, and guidelines for effective district management, supervision of credit unions, and quality assurance. The NSPM includes the NCUA's IT examination policies and procedures.
- **FFIEC Information Technology Booklets**: The FFIEC IT Handbook Infobase offers a variety of resources ranging from IT booklets and work programs to information on IT security-related laws, regulations, and guidance. Financial institutions can use these booklets to align their information security and cybersecurity practices with the FFIEC guidelines.
- **Credit Union Service Organization (CUSO) Reviews:** As discussed in more detail below, the NCUA lacks direct regulatory authority over CUSOs. Nevertheless, the NCUA and state supervisory authorities (under state statutes) periodically perform independent or joint reviews of CUSOs to verify the CUSO is complying with statutory and regulatory requirements. CUSOs may reject the recommendations of the NCUA because of the lack of vendor authority.

Information Technology and Cybersecurity Supervisory Guidance

The NCUA, in conjunction with other federal and state regulators, provides federally insured credit unions with a variety of supervisory guidance and resources related to IT security, as listed below.

- **Risk Alerts**: Risk alerts provide details on practices or external threats that are a potentially significant risk to the safety and soundness of the credit union system. A recent IT-related alert is included below.

- Heightened Risk of Social Engineering and Phishing Attacks: Reminds credit unions to remain vigilant in protecting against social engineering and phishing attacks.

- **Joint Agency Statements**: The FFIEC, on behalf of its members, issues statements to notify financial institutions of guidance, growing trends, best practices, cyberattacks, and other related risk and threats. The NCUA participated in the recent FFIEC statement on IT security listed below.
  - Cybersecurity Resource Guide for Financial Institutions: Updates the October 2018 Cybersecurity Resource Guide for Financial Institutions. The purpose of this guide is to help financial institutions meet their security control objectives and prepare to respond to cyber incidents.

Agency Cybersecurity Program

The NCUA Enterprise Risk Management Council has assessed the risk appetite for information and technology management at low for operational IT and IT systems. Like all federal agencies, the NCUA must comply with mandatory security standards for federal information and information systems.[3] The NCUA must meet these minimum information security requirements by using security and privacy controls recommended by the NIST and the Federal Information Security Modernization Act (FISMA).[4]

The NCUA employs a defense-in-depth approach to information and system security, using policy as the first tier of the NCUA's cyber-defense. The NCUA designed and disseminated fully developed agency-wide and program-specific policies and procedures to establish appropriate practices for collecting, securing, retaining, and destroying data. These policies and procedures are based on applicable requirements in information security laws, or are otherwise mandated by NIST, the Office of Management and Budget, the U.S. Department of Homeland Security (DHS), or the National Archives and Records Administration.

The NCUA has identified high value assets and critical system architecture to understand the potential impact to those assets from a cyber incident and ensure robust physical and cybersecurity protections are in place.

The NCUA implements applicable policies, statutes, and regulations using the NIST Risk Management Framework and adherence to NIST Special Publication 800-53 - *Security and*

[3] FIPS Publication 199, *Standards for Security Categorization of Federal Information and Information Systems*; FIPS Publication 200, *Minimum Security Requirements for Federal Information and Information Systems*.

[4] NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

Privacy Controls for Information Systems and Organizations.[5] The NCUA continuously complies with binding operational directives, emergency directives, and cybersecurity coordination, assessment and response directives issued by the DHS Cybersecurity and Infrastructure Security Agency (CISA).

The NCUA documents, categorizes, and authorizes all information systems in the enterprise, to include internally hosted federal systems, contractor-hosted systems, and services provided by third parties. As part of system authorization, the NCUA accounts for all information types, assets, and information systems; the roles and responsibilities of those who manage and operate them; and the interconnection of these systems and data. Based on information and system sensitivity, the NCUA selects security controls necessary to protect the confidentiality, integrity, and availability of the organizational security systems and critical infrastructure. The implementation statements related to selected security controls are designed, baselined, and tested to ensure they produce the desired outcome. Data is encrypted in transit and at rest.

Once authorized, systems are continuously monitored using automated and manual processes with regular testing of controls to validate their continued efficacy. Systems authorization data is stored in the NCUA's governance, risk, and compliance repository, which aggregates and analyzes enterprise risk information. This provides seamless reporting to DHS CISA.

Activities to Ensure Effective Information Technology Security

Appointing Qualified Staff

The NCUA has hired staff focused on cybersecurity and privacy. IT security staff hired include cyber security operations and incident responders, risk and compliance specialists, and network security engineers. In addition, the agency uses contract staff with specialized skills to support its work in the areas of:

- Computer forensics;
- Defensive cyber operations;

[5] In addition to NIST standards and guidelines, the NCUA is subject to federal statutes such as the Federal Information Security Modernization Act of 2014, the E-Government Act of 2002, the Privacy Act of 1974, and various Office of Management and Budget policies and guidance concerning federal information management and privacy.

- Malware analysis and mitigation;
- Security information and event management;
- Configuration and management;
- Threat hunting; and
- Incident handling and response.

The NCUA established an Enterprise Risk Management Council, a Cybersecurity Council, and an Information Technology Oversight Council. These collaborative groups are comprised of senior executives with diverse backgrounds, including IT, and are tasked with monitoring, measuring, managing, and prioritizing risks and related investments, including IT security. These councils meet as often as monthly and are briefed regularly on cyber-risk issues and events that relate to credit unions, financial services, or the agency.

The NCUA also has staff with requisite national security clearances to support the dissemination of classified information to appropriately cleared staff members on a need-to-know basis. The Chief Information Officer, the Senior Agency Information Security/Risk Officer, and the Senior Agency Official for Privacy collaborate to ensure compliance with regulation and drive security performance. To enhance the security of the NCUA's systems, an Information Systems Security Officer program was established in 2018 to provide specialized expertise to the NCUA offices involved in operating internal information systems.

Additionally, a Cybersecurity Adviser and Coordinator position was established in 2021 to organize, coordinate, and advise on cybersecurity and critical infrastructure matters across all NCUA offices. This includes supporting coordination and oversight for agency councils, working groups, special projects, security assessments, and incident responses related to cybersecurity and critical infrastructure. With respect to cybersecurity and critical infrastructure matters, the position will enhance the NCUA's contributions to and partnerships with other federal banking agencies, conduct stakeholder outreach and engagement, support NCUA staff training and development programs, help enhance the information and guidance provided to credit unions and other stakeholders, and assist in organizing special events and activities. The NCUA filled the position in early 2023.

Staff Training

The NCUA provides mandatory privacy and security awareness training to all NCUA system users. The training addresses appropriate information security practices, rules of behavior for access and use of data systems, responsibilities for protecting personally identifiable information,

and ethics rules prohibiting unauthorized information disclosures. Staff are trained on policies regarding:

- Collecting information necessary to perform their planned review;
- Collecting information in a secure manner using a hierarchy of secure methods that best suit the situation;
- Transferring and storing any sensitive information only where there is an identified, authorized need to retain such information, and in a manner consistent with agency instructions for handling sensitive information; and
- Destroying or returning all other non-public sensitive or personally identifiable information at the conclusion of the examination or review.

Staff who have elevated access to systems or have management responsibility for systems and data take mandatory role-based training. For NCUA staff serving in cybersecurity roles, individual development plans are developed collaboratively with managers to build domain-specific skills. At least 80 hours of instructor-led training or conferences are allocated annually for each person. All agency staff receive general and role-based training on information security and cybersecurity at least annually. This training addresses staff's legal, reputational, and ethical obligations to protect sensitive information.

Information Security Examination Training Program

The NCUA's information security examination training program includes classroom, online, and on-the-job training. The program is designed to specifically address competencies in the areas of IT, information security, and cybersecurity.

The program provides instruction on topics including NCUA regulations parts 748 and 749, agency guidance, and industry best practices related to measuring, monitoring, reporting, and controlling IT risks. Examiner training is designed to maintain and update knowledge of standards, tools, and practices to identify, detect, prevent, and mitigate IT and cybersecurity risks, threats, and vulnerabilities.

Examiners complete the principal examiner certification program, which includes a written knowledge test. The test requires the examiner to demonstrate proficiency in IT areas, including internal controls, risk assessments, information security policy, incident response, and business continuity planning.

The NCUA has a cadre of examiners specially trained on IT security and other examination positions that specialize in IT security reviews. These subject matter experts have the technical

knowledge and skills necessary to perform in-depth IT examinations. The NCUA also has highly specialized personnel in the Office of Examination and Insurance (E&I) to develop and maintain examination policies and tools, supervisory guidance, and examiner training. E&I coordinates with other supervisory agencies on IT security issues.

The NCUA has recently released its updated information security examination training program. The courses are designed to introduce information security examination procedures and expand examiners' understanding of cybersecurity concepts found in the FFIEC IT Booklets, the NIST cybersecurity standards, and industry best practices. Through this training, examiners will gain an understanding of how to perform an effective review of a credit union's information security program. In addition, examiners participate in on-the-job training and complete intermediate reviews under the guidance of an experienced specialized examiner.

Credit Union Training and Support

The NCUA provides training for credit unions. The NCUA's Office of Credit Union Resources and Expansion (CURE) has expanded educational opportunities for credit unions on the NCUA Learning Management Service platform. The learning management service is available to credit unions at no cost. In addition, CURE hosts webinars that deliver timely and meaningful information to help credit union professionals stay current on relevant topics affecting the credit union community. For example, CURE hosted a webinar in October 2022 entitled Ransomware in the Financial Sector. This webinar provided credit union management with important information on how to protect their credit unions and membership.

The NCUA provides credit unions additional resources through the NCUA website and by offering technical assistance grants and low-interest loans to low-income designated credit unions. Below are some other examples of credit union resources provided by the NCUA:

- **Modern Examination and Risk Identification Tool (MERIT)**: MERIT is the NCUA's examination tool, which replaced the agency's legacy examination platform. MERIT enables credit unions to:
    - Transfer files securely within the context of an examination;
    - Access status updates;
    - Request due date changes on examination findings and action items; and
    - Retrieve completed examination reports.
- **ACET Application**: ACET simplifies the process of determining a credit union's exposure to risk by identifying the type, volume, and complexity of the institution's operations, and enables the credit union to measure levels of risk and the adequacy of

corresponding controls. ACET is based on the DHS Cyber Security Evaluation Tool. It provides a multitude of cybersecurity standards and other resources for a credit union to conduct self-assessments, including the Ransomware Readiness Assessment. As of May 2023, the application has been downloaded 9,063 times.

- **NCUA Website**: The NCUA website provides cybersecurity resources for research and informational purposes. Specifically, the Cybersecurity Resources page contains applicable references to NCUA regulations and guidance, federal government requirements and guidelines, information sharing, cyber threats, best practices, and privacy and protection.

- **Grants and Loans**: The NCUA provides technical assistance grants and low-interest loans to support credit unions' efforts to improve and expand service through the Community Development Revolving Loan Fund (CDRLF). Year after year, demand for CDRLF funding continues to exceed supply. During the 2022 grant round, the agency received 220 applications totaling more than $4.7 million and awarded more than $1.5 million in technical assistance grants to 90 low-income-designated credit unions. Of that amount, 52 grants totaling $484,165 were specifically for digital services and cybersecurity projects.

Agency Investment in Information Technology Security

The NCUA has invested significant resources in its network and security infrastructure. These investments are designed to deny access or prevent efforts to degrade, disrupt, or destroy any NCUA information and information system or network, or exfiltrate NCUA information from systems or networks without authorization.

All basic user accounts are required to use multi-factor, certificate-based authentication to access network resources. Elevated privilege accounts (system and network administrators and engineers) are issued session-based credentials with specific expiration timeframes. To mitigate vulnerabilities, NCUA network users remotely accessing network services and resources are protected by encrypted virtual private network (VPN) tunnels, and internal and external network traffic is managed and monitored. VPN connectivity on NCUA laptops is mandatory for all users. This continually enforces technical policies and ensures traffic and data are encrypted and secure.

To enhance visibility into network and infrastructure operations and observable anomalous behaviors, the NCUA procured, implemented, and optimized a security information and event management solution. The NCUA also leverages DHS's EINSTEIN infrastructure and Trusted Internet Connection (TIC) 3.0 to enhance cybersecurity analysis, situational awareness, and security response in internet traffic and connections.

The NCUA's approach to data loss prevention is to limit local downloading of business information to centrally tracked and managed encrypted devices. For email data loss and exfiltration, the NCUA procured a third-party technology that monitors, notifies, logs, and prevents business information from malicious and inadvertent transfer to external email domains. For endpoint malware-based data exfiltration, the NCUA procured a robust real-time Endpoint Detection and Response tool with integrated open-source intelligence feeds creating opportunity for malware auto-response at the user and server endpoints.

To mitigate risks resulting from infrastructure failure, the NCUA has redundant data center facilities that are failovers for key NCUA network resources and services. Key public-facing web services have been migrated to cloud-based infrastructure to leverage both inherent geographic dispersion and infrastructure failure risk mitigation. For critical business productivity and collaboration client resilience, the NCUA migrated to Microsoft's Office 365 environment.

As part of the initiative to move to a zero-trust architecture and accelerate movement to secure cloud services, the NCUA is carefully evaluating the need for additional investment in both technology and personnel.

Finally, the NCUA evaluates new systems and services to determine if they are candidates for the Office of Management and Budget's Cloud Smart initiative.

Audits and Reviews of the NCUA's Cybersecurity Program

The NCUA's Office of the Inspector General (OIG) conducts independent audits, investigations, and other activities to verify the NCUA's compliance with applicable standards, laws, and regulations — including those related to privacy and information security — to determine whether the NCUA effectively implemented all appropriate security and privacy controls.

As a result of these audits, the NCUA receives and manages notices of findings and recommendations (NFRs). These notices are the subject of plans of action and milestones and are systematically remediated over time.

In addition, as indicated in the Financial Statement Audits, the NCUA complies with the requirements of the Federal Managers' Financial Integrity Act of 1982.6 The results are reported both internally and externally to ensure completion of all remedial findings. Credit unions and their members can review OIG audit reports, semiannual reports, and letters to Congress at https://www.ncua.gov/About/Pages/inspector-general/reports.aspx.

[6] https://www.congress.gov/97/statute/STATUTE-96/STATUTE-96-Pg814.pdf

NCUA senior leadership are briefed on NFR status on a quarterly basis, and resources are allocated as appropriate to ensure mitigation. The NCUA Board is briefed on the FISMA audit and Federal Information System Controls Audit Manual results and on remediation activities by both the Executive Director's office and the Chief Information Officer. There are five maturity levels, and the NCUA is graded as Maturity Level 4 "Managed and Measurable." This rating reflects that the NCUA's information security program is effective and the agency can demonstrate this quantitatively and qualitatively.

Industry Response to Regulator's Efforts

In response to the policies, procedures, and activities making up the NCUA's IT examination program, credit unions have significantly improved their IT programs. Over the last 4 years, IT risk factors requiring immediate attention (which are issued to credit unions in the form of documents of resolution) have decreased.

The credit union system has responded positively to the efforts of the financial regulators by incorporating regulators' recommendations and guidance into private sector initiatives including:

- **Information Sharing and Analysis Organizations**: Credit unions have continued to voluntarily participate in information sharing organizations, such as the Financial Services Information Sharing and Analysis Center. Additionally, the National Credit Union Information Sharing and Analysis Organization was established as an Information Sharing and Analysis Organization specifically tailored to credit unions.
- **Hamilton Series Exercises**: The NCUA supports the U.S. Department of the Treasury-led Hamilton Series exercises to develop 1-day exercises aimed at improving the cyberthreat response within the U.S. financial sector. Simulations mimic a variety of cyberattacks. Participants include members of both the public and private sectors, so that results can be formed into improved public-private coordination strategies.
- **Sheltered Harbor**: As a result of the recommendations in a Hamilton Series exercise, the private sector developed Sheltered Harbor standards. These standards may assist some institutions in reconstituting certain data types after a catastrophic event.

Regulatory Coordination Efforts

The NCUA coordinates with other federal regulatory agencies to strengthen cybersecurity, including the development and dissemination of best practices and sharing threat information.

FFIEC: 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 NCUA,

the Board of Governors of the Federal Reserve System, the Federal Deposit Insurance Corporation, the Office of the Comptroller of the Currency, the Consumer Financial Protection Bureau, and the State Liaison Committee.

FFIEC Task Force on Supervision (TFOS): The TFOS coordinates and oversees matters relating to safety and soundness supervision and examination of depository institutions. It provides a forum for the financial regulators to promote quality, consistency, and effectiveness in examination and supervisory practices and to reduce unnecessary regulatory burden on those institutions. The NCUA also has representation on the two subcommittees of the TFOS:

- **Information Technology Subcommittee**: This forum addresses information systems and technology policy issues as they relate to financial institutions and their technology service providers.
- **Cybersecurity and Critical Infrastructure Working Group**: This working group addresses policy relating to cybersecurity, critical infrastructure security, and the resilience of financial institutions and technology service providers.

Financial Stability Oversight Council (FSOC): The NCUA Chairman is a voting member of the FSOC. The FSOC is charged with:

- Identifying risks, including IT, to the financial stability of the United States;
- Promoting market discipline; and
- Responding to emerging risks to the stability of the United States' financial system.

The Council consists of 10 voting members and 5 nonvoting members and brings together the expertise of federal financial regulators, state regulators, and an independent insurance expert appointed by the President.

Financial and Banking Information Infrastructure Committee (FBIIC): The NCUA is one of the 18 FBIIC member organizations from across the financial regulatory community, both federal and state. The FBIIC is chaired by the U.S. Department of the Treasury and chartered under the President's Working Group on Financial Markets, which was established by Executive Order 12631. Working with members from the financial regulatory agencies, the FBIIC coordinates efforts to improve the reliability and security of the financial sector infrastructure.

Through monthly meetings, staff from FBIIC member organizations work on operational and tactical issues related to critical infrastructure matters, including cybersecurity, within the financial services industry. The FBIIC also leads the financial sector's cybersecurity exercises. In 2021, the NCUA and the U.S. Department of the Treasury held an exercise specifically for credit unions, which simulated a third-party compromise.

Financial Services Sector Coordinating Council (FSSCC): The NCUA collaborates and coordinates with the private sector through the FSSCC. The FSSCC was established in 2002 by the financial sector to work collaboratively with key government agencies to protect the nation's critical infrastructure from cyber and physical threats. The mission of the FSSCC is to strengthen the resiliency of the financial services sector against attacks and other threats to the nation's critical infrastructure by proactively identifying threats and promoting protection, driving preparedness, collaborating with the U.S. federal government, and coordinating crisis response for the benefit of the financial services sector, consumers, and the United States. The FSSCC is comprised of more than 70 members from financial trade associations, financial utilities, and the most critical financial firms. Through government relationships, the FSSCC directly assists the sector's response to natural disasters.

Federal Agency Coordination

As a federal agency, the NCUA follows the DHS CISA and U.S. Department of the Treasury direction during government-wide incident response activities. In addition, the NCUA identifies potential, actual, and emerging threats, issues, or challenges to analyze underlying causes and develop innovative short- and long-term solutions. This analysis supports the shaping of the NCUA's internal policies and procedures related to cybersecurity, critical infrastructure protection, supply chain risks, national security, insider threats, counterintelligence, continuity of operations, and emergency response.

The NCUA staff also participate in interagency initiatives, including:

- DHS CISA security operations center information and collaboration sessions;
- Treasury sector cybersecurity collaboration and information sessions;
- The Federal Chief Information Security Officer Council; and
- The Small Agency Chief Information Security Officer collaboration forum.

Current and Emerging Threats

Threats to the Financial Sector

The NCUA remains concerned about the risks cyberattacks pose to the financial system. Cybersecurity risks grow as threats evolve, become more sophisticated, and cause damage to a variety of industries. Geopolitical tensions increase the possibility of nation-states and other sophisticated actors conducting malicious cyberattacks against U.S. critical infrastructure—of

which credit unions are a vital part. Credit unions must implement appropriate controls to use technology, deliver member services, and adopt financial innovation, to ensure the industry's long-term success, safely and securely. The likelihood of these threats adversely affecting credit unions and their members continues to rise in correlation to the advances and adoption of financial technology.

More specifically, current and emerging cybersecurity threats to credit unions include:

- **Geopolitical Tensions**: Given current geopolitical threats, the NCUA, along with CISA, the Federal Bureau of Investigation, and the National Security Agency encouraged credit unions of all sizes and their cybersecurity teams nationwide to adopt a heightened state of awareness and to conduct proactive threat hunting. The NCUA provided guidance and resources to credit unions to assist in mitigating this threat. As part of this guidance, the NCUA recommended credit unions report cyber incidents to DHS CISA and directed credit unions to the Shields Up website for additional information and mitigation measures.
- **Ransomware**: Ransomware remains the most immediate threat to credit unions. Many ransomware operations now integrate extortion in data theft campaigns. Ransomware attacks continue across all sectors and companies, including the financial sector, and have left business processes and organizations without the data they need to operate. To increase pressure on organizations to satisfy extortion demands, cyber intruders now demand payment in exchange for not releasing sensitive information obtained during a cyberattack. Ransomware has evolved to ransomware as a service, whereby multiple intruders coordinate their activities to conduct a single intrusion event, making it more challenging for financial institutions to defend against such attacks.
- **Supply Chain**: Supply chain risk continues to increase and evolve with attacks that target vulnerabilities in software systems commonly used by large numbers of credit unions. Threat actors exploit vulnerabilities in third-party hardware and software systems to conduct malicious cyber activities.

  These attacks demonstrate the importance of credit unions assessing the risks posed by third- party vendors, inclusive of the supply chain, and developing a comprehensive approach to operational resilience.
- **Third-Party Risk**: Cyber actors also continue to increase their efforts to exploit vulnerabilities of third-party providers. As an associated aspect of supply chain risk, third-party risks continue to be an area of heightened supervisory focus for the NCUA.

The number of credit unions using IT service providers, such as managed and cloud services, has dramatically increased in recent years because IT service providers enable credit unions to more

cost effectively scale and support network environments. By servicing large numbers of customers, IT service providers can achieve significant economies of scale. However, outsourcing processes or functions does not eliminate credit union responsibility for the safety, security, and soundness of those processes and functions.

Over time, there has also been a consolidation of technology service providers which increases the concentration risk for the credit union system. As of June 2023, the top five credit union core processing system third-party vendor categories (data processing, audit, eWeb, account verification, and Bank Secrecy Act) provide service to credit unions holding approximately 87 percent of total federally insured credit union industry assets. When there is an incident at a third party that only services credit unions, such as a CUSO, the federal banking agencies do not have regulatory authority. Therefore, neither the NCUA nor the banking agencies receives notification of the incident, and both would be unable to determine the impact of the incident on the entire financial sector and take timely remedial action.

Throughout 2022, incidents at vendors accounted for approximately 27 percent of total incidents. As NCUA does not have third-party vendor authority, the agency is unable to validate whether mitigating controls have been adequately implemented to prevent a recurrence of these specific incidents or to ensure adequate controls are in place to identify, monitor, and prevent new incidents from occurring.

The NCUA's Lack of Vendor Authority

Currently, unlike all other federal banking regulators, the NCUA has no authority over third-party service providers and only a limited ability to provide oversight of the services provided by CUSOs. The NCUA has requested the restoration of statutory authority over third-party vendors, including CUSOs. Specifically, the NCUA is seeking examination authority over CUSOs, whether wholly or partially owned by federally insured credit unions, and examination authority over third-party service providers.

In March 2022, the NCUA published a paper on Third-Party Vendor Authority that outlines significant risks and challenges presented by the NCUA's lack of authority over third-party vendors, including CUSOs, that provide services to federally insured credit unions. The paper stated that this growing regulatory blind spot has the potential to trigger cascading consequences throughout the credit union industry and the financial services sector, which may result in significant losses to the NCUSIF, which is backed by the full faith and credit of the U.S. government.

The paper also highlighted that some third-party vendors may pose a national security risk to the United States due to a lack of oversight and enforcement authority over their business operations. This risk is primarily a cybersecurity risk, given the amount and type of data they hold, as well as

business functions they perform for federally insured credit unions. Roughly one in three Americans have a financial relationship with a credit union, so the risks introduced into the system have consequences for a broad segment of the financial system.

Increasingly, activities that are fundamental to the credit union mission, such as loan origination, lending services, Bank Secrecy Act/Anti-Money Laundering compliance, and financial management, are being outsourced to entities that are beyond the purview of the NCUA's supervisory oversight. In addition, credit unions are increasingly using third-party vendors to provide technological services, including information security and mobile and online banking, and store member data. The pandemic, which has accelerated the industry's movement to digital services, has increased credit union reliance on third-party vendors.

While there are many advantages to using these service providers, it is important to recognize the potential safety and soundness and compliance risk posed by the concentration of credit union services within CUSOs and third-party vendors. For example, the top five CUSOs provide services to nearly 96 percent of total credit union system assets. The top five credit union core processor vendors provide services to approximately 87 percent of total credit union system assets. A security, operational, or financial failure of even one of these vendors represents a significant potential risk to the credit union industry.

Given the continued transfer of operations to CUSOs and other third parties in the credit union system, the NCUA's lack of third-party vendor authority limits the NCUA's ability to accurately assess all the risks present in the credit union system and determine whether current CUSO or third-party vendor risk-mitigation strategies are adequate. That is one of the reasons why the FSOC, the Government Accountability Office, and the NCUA's Inspector General have each called on Congress to close this growing regulatory blind spot. The current NCUA Chairman, along with other recent chairmen, has requested legislative action to restore the NCUA's vendor authority. In addition, in the preamble to the October 2021 Credit Union Service Organizations final rule, the NCUA Board reaffirmed that "it is the Board's continuing policy to seek third-party vendor authority for the agency from Congress."

Agency Cybersecurity Threats

Phishing email messages continue to be the primary source of malicious links and documents for the NCUA. To help mitigate the risk of successful attacks, the NCUA conducts quarterly phishing exercises to test NCUA users' ability to identify and report suspicious messages. The NCUA implemented technology to protect staff from email phishing attempts, as well as hyperlinks, websites, and email attachments that contain malicious software.

The NCUA also implemented a cloud-based service to evaluate the risk third parties may pose to the data and systems utilized for essential functions of its business.

Conclusion

The NCUA continues to promote cybersecurity best practices in credit unions, and reviews of credit union information systems and assurance programs remain a supervisory priority for the agency. Building upon its industry outreach efforts, the NCUA will continue to provide guidance and resources to assist credit unions with strengthening their cyber defenses throughout the year. As part of its 2023 grant initiative, the agency is again funding cybersecurity grants.

The NCUA is also examining ways to strengthen cybersecurity reviews during regular examinations of credit unions and is updating its information security examination program to better reflect current cybersecurity risks.

Internally, the NCUA maintains strong resilience in network and security infrastructure designed to deny access to or prevent efforts to degrade, disrupt, or destroy any NCUA information and information system or network, or exfiltrate NCUA information from systems or networks without authorization.

Finally, the NCUA's lack of third-party vendor authority is a growing regulatory blind spot for the agency and the broader financial system, posing a cybersecurity, national security, money laundering, compliance, and reputation risk to the agency from consumer loss of confidence in the industry. The agency supports legislation to restore the authority that expired on December 31, 2001.

Appendix: Resources

Laws, Regulations, and Reports

Source:	Reference:	Impact:
NCUA	Part 748 – Security Program	IT Examination
NCUA	Part 749 – Records Preservation Program	
FTC	Gramm-Leach-Bliley Act, Safeguards Rule	
OIG Report	OIG-17-08, Audit of the NCUA Information Technology Examination Program	Cybersecurity
OIG Report	OIG-19-07, Audit of the NCUA Office of National Examinations and Supervision Oversight of Credit Union Cybersecurity Programs	
OIG Report	OIG-20-07, Audit of the NCUA's Examination and Oversight Authority Over Credit Union Service Organizations and Vendors	
Executive Order	Consolidated Appropriations Act, 2021 (House Committee Print 116-68)	

Recent NCUA Letters to Credit Unions

Year:	Letter:	Letters to Credit Unions:
2022	22-CU-07	Federally Insured Credit Union Use of Distributed Ledger Technologies
2021	21-CU-16	Relationships with Third Parties that Provide Services Related to Digital Assets
2021	21-CU-15	Automated Cybersecurity Evaluation Toolbox
2017	17-CU-08	Interagency Supervisory Guidance for Institutions Affected by a Major Disaster

NCUA Risk Alerts

Year:	Reference:	Alert:
2022	22-RISK-01	Heightened Risk of Social Engineering and Phishing Attacks
2022	CISA	Cyber Actors Targeting Ubiquitous Log4j Vulnerability
2021	21-RISK-01	Business Email Compromise through Exploitation of Cloud-Based Email Services
2020	20-RISK-02	Cybersecurity Considerations for Remote Work
2019	19-RISK-01	Business Email Compromise Fraud

NCUA Supervisory Priorities

Year:	Letter:	Reference:
2023	23-CU-01	NCUA's 2023 Supervisory Priorities
2022	22-CU-02	NCUA's 2022 Supervisory Priorities
2021	21-CU-02	NCUA's 2021 Supervisory Priorities
2020	20-CU-22	Update to NCUA's 2020 Supervisory Priorities
2020	20-CU-01	2020 Supervisory Priorities
2019	19-CU-01	Supervisory Priorities for 2019
2017	17-CU-09	Supervisory Priorities for 2018

NCUA Exam Guide / National Supervision Policy Manual (NSPM)

Reference:	Resource:
Examiner's Guide	Risk-Focused Examinations
NSPM	NSPM Public v20.0

NCUA Joint Statement Cybersecurity Press Releases

Date:	Press Release:
8/11/2021	Authentication and Access to Financial Institution Services and Systems
3/29/2021	Agencies Seek Wide Range of Views on Financial Institutions' Use of Artificial Intelligence
4/30/2020	FFIEC Issues Statement on Risk Management for Cloud Computing Services
3/6/2020	FFIEC Highlights Pandemic Preparedness Guidance
11/14/2019	Financial Regulators Revise Business Continuity Management Booklet to Stress to Examiners the Value of Resilience to Avoid Disruptions to Operations
8/28/2019	FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness
11/27/2018	FFIEC Emphasizes Risk-Focused Supervision in Second Update of the Examination Modernization Project
9/11/2018	Agencies Issue Statement Reaffirming the Role of Supervisory Guidance
4/10/2018	FFIEC Issues Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs
3/22/2018	FFIEC Provides Update of Examination Modernization Project

FFIEC IT Booklets

Release Date:	Reference:	Booklet:
6/2021	FFIEC IT Booklet	Architecture, Infrastructure, and Operations
11/2019	FFIEC IT Booklet	Business Continuity Management
9/2016	FFIEC IT Booklet	Information Security
4/2016	FFIEC IT Booklet	Retail Payment Systems
11/2015	FFIEC IT Booklet	Management
10/2012	FFIEC IT Booklet	Supervision of Technology Service Providers
6/2004	FFIEC IT Booklet	Outsourcing Technology Services
6/2004	FFIEC IT Booklet	Wholesale Payment Systems

FFIEC Cybersecurity Awareness: Resources

Resource:
FFIEC Cybersecurity Resource Guide for Financial Institutions
FFIEC Authentication and Access to Financial Institution Services and Systems Guidance
FFIEC Statement on Security in a Cloud Computing Environment
FFIEC Office of Foreign Assets Control Cyber-Related Sanctions Program Risk Management
FFIEC Statement on Cyber Insurance and Its Potential Role in Risk Management Programs
FFIEC Cybersecurity Assessment Tool Frequently Asked Questions
Cybersecurity of Interbank Messaging and Wholesale Payment Networks
FFIEC Cybersecurity Assessment Tool Presentation
FFIEC Statement on Destructive Malware
FFIEC IT Examination Handbook InfoBase
Introduction to the FFIEC's Cybersecurity Assessment
FFIEC Cybersecurity Assessment General Observations
Cybersecurity of Interbank Messaging and Wholesale Payment Networks

Resource:
FFIEC Cybersecurity Assessment Tool Presentation
Webinar: Executive Leadership of Cybersecurity

FFIEC Cybersecurity Awareness: Statements and Alerts Regarding Threats and Vulnerabilities

Date:	Statements:
4/30/2020	FFIEC Issues Statement on Risk Management for Cloud Computing Services
8/28/2019	FFIEC Encourages Standardized Approach to Assessing Cybersecurity Preparedness
11/5/2018	FFIEC Releases Statement on OFAC Cyber-Related Sanctions
4/10/2018	FFIEC Issues Joint Statement on Cyber Insurance and Its Potential Role in Risk Management Programs
5/31/2017	FFIEC Release Update to Cybersecurity Assessment Tool