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

As of June 30, 2021

NATIONAL CREDIT UNION ADMINISTRATION

NCUA

1934

NCUA
National Credit Union Administration

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 Share Insurance Fund provides up to at least $250,000 of federal share insurance to nearly 126 million members in all federal credit unions and most state-chartered credit unions. The NCUA is responsible for the federal regulation and supervision of 5,068 federally insured credit unions with more than $1.95 trillion in assets across all states and U.S. territories.

The NCUA also plays a role in helping to ensure broader financial stability as the current chair of the Federal Financial Institutions Examination Council (FFIEC) and as a member of the Financial and Banking Information Infrastructure Committee (FBIIC). The NCUA's Chairman is also 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. Due to vulnerabilities within the credit union industry and the broader financial system to potential cyberattacks, cybersecurity is one of the NCUA's top supervisory priorities and 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 our examination program and providing credit unions with guidance, information, and resources. The NCUA also continuously seeks to improve the security of agency systems and the information collected.

Credit unions require sound controls to safeguard against fraud, financial crimes, and operational errors. Regulatory and supervisory expectations for credit unions are designed to ensure they maintain comprehensive and operational resilience, commensurate with the size, scope, and complexity of products, services, and operations being offered by the institution. Ongoing monitoring and adjusting of internal controls, risk-management practices, and risk-mitigation strategies that adapt to the increasingly complex technology infrastructure and cybersecurity landscape are critical to achieving operational resiliency. To remain competitive, credit unions must be able to safely and securely use technology to deliver member services 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 of 2021. 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 Technology 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. Various other laws provide the NCUA with authority and direction to regulate credit unions as well.

In particular, the Gramm-Leach-Bliley Act (GLBA) 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 any 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 that could result in substantial harm or inconvenience to any member.

In implementing the GLBA requirements, the NCUA issued 12 C.F.R. § 748, Appendix A, Guidelines for Safeguarding Member Information. These requirements govern what federally insured credit unions must do to develop an information security program designed to ensure the security and confidentiality of member records, protect against the anticipated threats or hazards to the security or integrity of such records, and safeguard against unauthorized access to or use of such records that could result in substantial harm or serious inconvenience to a member. This regulation also contains requirements for credit unions to notify the NCUA of certain information security incidents.

Information Technology and Cybersecurity Examination

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.

All federally insured credit unions receive an NCUA examination on a periodic basis.[1] To ensure both compliance with applicable laws and regulations, and safety and soundness, a review of the credit union's information technology (including components of information security and cybersecurity) is performed at each examination. The NCUA uses a risk-focused approach to examine credit unions' information technology to provide examiners flexibility to focus on areas of material current or potential risk relevant to each credit union's unique business model and information technology. The objectives of information technology examination procedures include:

- 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 information technology operations.
- Determining whether the board of directors has adopted and implemented adequate information technology-related policies and procedures.
- Evaluating the adequacy of internal information technology controls and oversight to safeguard member information.

[1] 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.

The NCUA's information technology examination program incorporates the following:

- Automated Cybersecurity Examination Tool (ACET): The ACET allows the NCUA and credit unions to determine the maturity of a credit union's information security program. The tool incorporates appropriate cybersecurity standards and practices established for financial institutions. The tool maps each of its declarative statements to the practices found in the FFIEC IT Examination Handbook, regulatory guidance, and leading industry standards like the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF). The tool also provides examiners a plain-language explanation and references for each of the statements included within the assessment.
- Information Technology Risk Examination for Credit Unions (InTREx-CU): The NCUA has been piloting InTREx-CU, an enhanced approach for conducting information technology examinations. InTREx-CU will be fully deployed for examinations starting in 2022.
- 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 information technology 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, including as it relates to the NCUA's information technology 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 Unions Service Organization (CUSO) Reviews: Although (as discussed in more detail below) the NCUA lacks direct regulatory authority over CUSOs, the NCUA and State Supervisory Authorities (under state statutes) periodically perform independent or joint reviews of CUSOs to ensure they comply with statutory and regulatory requirements. These reviews are also designed to ensure that CUSOs use sound business and operational practices and to determine whether the CUSO complies with statutory and regulatory requirements for the products and services they provide.

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 information technology security. These include the following:

- Letters to Credit Unions: Letters to Credit Unions provide guidance on specific NCUA policies and procedures, compliance, governance, and other timely issues that affect all federally insured credit unions. Either through a Letter to Credit Unions or posting directly on the NCUA's website, the NCUA also shares most examiner guidance with the public. (Refer to Appendix).
- Risk Alerts: Risk alerts detail practices or external threats that are a potentially significant risk to the safety and soundness of the credit union system. Relevant recent alerts include:
    - Cybersecurity Considerations for Remote Work: Highlights cybersecurity best practices for credit unions that leverage employees' personal networks and devices.
    - Business Email Compromise Fraud: Describes the increasing frequency of and losses related to business email compromise fraud schemes.
    - Mitigating Distributed Denial-of-Service Attacks: Identifies appropriate policies and procedures to guard against distributed denial-of-service attacks.
    - Raising Consumer Awareness of Phishing Schemes: Raises consumer awareness on phishing schemes and informs consumers of steps NCUA has taken to combat this threat.
- 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. For information technology security, the NCUA participated in the following recent FFIEC statements:
    - FFIEC Joint Statement on Cyber Attacks Involving Extortion: Notifies financial institutions of the increasing frequency and severity of cyberattacks involving extortion.
    - FFIEC Statement on Destructive Malware: Notifies financial institutions of the increasing threat of cyberattacks involving destructive malware.
    - FFIEC Statement on Compromising Credentials: Notifies financial institutions of the growing trend of cyberattacks for the purpose of obtaining online credentials for theft, fraud, or business disruption and recommends risk mitigation techniques.

NCUA’s Information Technology Security

Like all federal agencies, the NCUA must comply with mandatory security standards for federal information and information systems.[2] The NCUA Enterprise Risk Management Committee (ERMC) has established the risk appetite for Information and Technology Management at LOW for operational information technology/information technology systems and MODERATE for non-production innovation. The NCUA must meet these minimum information security requirements by using security and privacy controls recommended by the National Institute of Standards and Technology.[3]

The NCUA employs a defense-in-depth approach to information and system security, utilizing 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 Department of Homeland Security, or the National Archives and Records Administration. The NCUA implements applicable policies, statutes, and regulations using the NIST Risk Management Framework and adherence to NIST Special Publication 800-53 revision (5) - Security and Privacy Controls for Information Systems and Organizations.[4] The NCUA documents, categorizes, and authorizes all information systems in the enterprise.

The NCUA is also required to adhere to the NIST Cyber Security Framework (CSF) standards, guidelines, and best practices for managing cybersecurity-related risk to include the appropriate implementation of the following (18) Security Control Families and their associated (256) controls:[5]

- **Access Control (AC):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (AC-1) Access Control Policy and Procedure; (AC-2) Account Management; (AC-3)

[2] 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.

[3] NIST Special Publication 800-53 (Rev. 5), Security and Privacy Controls for Federal Information Systems and Organizations.

[4] 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 (OMB) policies and guidance concerning federal information management and privacy.

[5] NIST Cybersecurity Framework, Federal Framework for Critical Infrastructure and Other Sectors Associated with the Economy and National Security.

Access Enforcement; (AC-4) Information Flow Enforcement; (AC-5) Separations of Duties; (AC-6) Least Privilege; (AC-7) Unsuccessful Logon Attempts; (AC-8) System Use Notification; (AC-9) Previous Logon (Access) Notification; (AC-10) Concurrent Session Control; (AC-11) Session Lock; (AC-12) Session Termination; (AC-13) Supervision and Review for Access Control; (AC-14) Permitted Actions Without Identification or Authentication; (C-15) Automated Marking; (AC-16) Security Attributes; (AC-17) Remote Access; (AC-18) Wireless Access; (AC-19) Access Control for Mobile Devices; (AC-20) Use of External Information Systems; (AC-21) Information Sharing; (AC-22) Publicly Accessible Content; (AC-23) Data Mining Protection; (AC-24) Access Control Decisions; and (AC-25) Reference Monitor.

- **Awareness and Training (AT):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (AT-1) Security Awareness and Training Policy and Procedures; (AT-2) Security Awareness Training; (AT-3) Role-Based Security Training; (AT-4) Security Training Records; and (AT-5) Contacts with Security Groups and Associations.
- **Audit and Accountability (AU):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (AU-1) Audit and Accountability Policy and Procedures; (AU-2) Audit Events; (AU-3) Content of Audit Records; (AU-4) Audit Storage Capacity; (AU-5) Response to Audit Processing Failures; (AU-6) Audit Review, Analysis and Reporting; (AU-7) Audit Reduction and Report Generation; (AU-8) Time Stamps; (AU-9) Protection of Audit Information; (AU-0) Non-Repudiation; (AU-11) Audit Record Retention; (AU-12) Audit Generation; (AU-13) Monitoring for Information Disclosure; (AU-14) Session Audit; (AU-15) Alternate Audit Capability; and (AU-16) Cross-Organizational Auditing.
- **Security Assessment and Authorization (CA):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (CA-1) Security Assessment and Authorization Policy and Procedures; (CA-2) Security Assessments; (CA-3) System Interconnections; (CA-4) Security Certifications; (CA-5) Plans of Action and Milestones; (CA-6) Security Authorization; (CA-7) Continuous Monitoring; (CA-8) Penetration Testing; and (CA-9) Internal System Connections.
- **Configuration Management (CM):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (CM-1) Configuration Management Policy and Procedures; (CM-2) Baseline Configuration; (CM-3) Configuration Change Control; (CM-4) Security Impact Analysis; (CM-5) Access Restrictions for Change; (CM-6) Configuration Settings; (CM-7) Least Functionality; (CM-8) Information System Component Inventory; (CM-9)

Configuration Management Plan; (CM-10) Software Usage Restrictions; and (CM-11) User-Installed Software.

- **Contingency Planning (CP):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (CP-1) Contingency Planning Policy and Procedures; (CP-2) Contingency Plan; (CP-3) Contingency Training; (CP-4) Contingency Plan Testing; (CP-5) Contingency Plan Update; (CP-6) Alternate Storage Site; (CP-7) Alternate Processing Site; (CP-8) Telecommunications Services; (CP-9) Information System Backup; (CP-10) Information System Recovery and Reconstitution; (CP-11) Alternate Communications Protocols; (CP-12) Safe Mode; and (CP-13) Alternative Security Mechanisms.
- **Identification and Authentication (IA):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (IA-1) Identification and Authentication Policy and Procedures; (IA-2) Identification and Authentication (Organizational Users); (IA-3) Device Identification and Authentication; (IA-4) Identifier Management; (IA-5) Authenticator Management; (IA-6) Authenticator Feedback; (IA-7) Cryptographic Module Authentication; (IA-8) Identification and Authentication (Non-organizational Users); (IA-9) Service Identification and Authentication; (IA-10) Adaptive Identification and Authentication; and (IA-11) Re-Authentication.
- **Incident Response (IR):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (IR-1) Incident Response Policy and Procedures; (IR-2) Incident Response Training; (IR-3) Incident Response Testing; (IR-4) Incident Handling; (IR-5) Incident Monitoring; (IR-6) Incident Reporting; (IR-7) Incident Response Assistance; (IR-8) Incident Response Plan; (IR-9) Information Spillage Response; and (IR-10) Integrated Information Security Analysis.
- **Maintenance (MA):** NCUA leverages this control family to address the establishment of policy, procedures and practices for the effective implementation and operations of (MA-1) System Maintenance Policy and Procedures; (MA-2) Controlled Maintenance; (MA-3) Maintenance Tools; (MA-4) Non-Local Maintenance; (MA-5) Maintenance Personnel; and (MA-6) Timely Maintenance.
- **Media Protection (MP):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (MP-1) Media Protection Policy and Procedures; (MP-2) Media Access; (MP-3) Media Marking; (MP-4) Media Storage; (MP-5) Media Transport; (MP-6) Media Sanitization; (MP-7) Media Use; and (MP-8) Media Downgrading.

- **Physical and Environmental Protection (PE):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (PE-1) Physical and Environmental Protection Policy and Procedures; (PE-2) Physical Access Authorizations; (PE-3) Physical Access Control; (PE-4) Access Control for Output Devices; (PE-6) Monitoring Physical Access; (PE-7) Visitor Control; (PE-8) Visitor Access Records; (PE-9) Power Equipment and Cabling; (PE-10) Emergency Shutoff; (PE-11) Emergency Power; (PE-12) Emergency Lighting; (PE-13) Fire Protection; (PE-14) Temperature and Humidity Controls; (PE-15) Water Damage Protection; (PE-15) Water Damage Protection; (PE-16) Delivery and Removal; (PE-17) Alternate Work Site; (PE-18) Location of Information System Components; (PE-19) Information Leakage; and (PE-20) Asset Monitoring and Tracking.
- **Planning (PL):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (PL-1) Security Planning Policy and Procedures; (PL-2) System Security Plan; (PL-3) System Security Plan Update; (PL-4) Rules of Behavior; (PL-5) Privacy Impact Assessment; (PL-6) Security-Related Activity Planning; (PL-7) Security Concept of Operations; (PL-8) Information Security Architecture; and (PL-9) Central Management.
- **Personnel Security (PS):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (PS-1) Personnel Security and Policy and Procedures; (PS-2) Position Risk Designation; (PS-3) Personnel Screening; (PS-4) Personnel Termination; (PS-5) Personnel Transfer; (PS-6) Access Agreements; (PS-7) Third-Party Personnel Security; and (PS-8) Personnel Sanctions.
- **Risk Assessment (RA):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (RA-1) Risk Assessment Policy and Procedures; (RA-2) Security Categorization; (RA-3) Risk Assessment; (RA-4) Risk Assessment Update; (RA-5) Vulnerability Scanning; (RA-6) Technical Surveillance Countermeasures Survey.
- **System and Services Acquisitions (SA):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (SA-1) System and Services Acquisition Policy and Procedures; (SA-2) Allocation of Resources; (SA-3) System Development Life Cycle; (SA-4) Acquisition Process; (SA-5) Information System Documentation; (SA-6) Software Usage Restrictions; (SA-7) User-Installed Software; (SA-8) Security Engineering Principles; (SA-9) External Information System Services; (SA-10) Developer Configuration Management; (SA-11) Developer Security Testing and Evaluation; (SA-12) Supply Chain Protection; (SA-13) Trustworthiness; (SA-14) Criticality Analysis; (SA-15) Development Process, Standards and Tools; (SA-16) Developer-Provided Training; (SA-

17) Developer Security Architecture and Design; SA-18) Tamper Resistance and Detection; (SA-19) Component Authenticity; (SA-20) Customized Development of Critical Components; (SA-21) Developer Screening; and (SA-22) Unsupported System Component.

- **System and Communications Protection (SC):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (SC-1) System and Communications Protection Policy and Procedures; (SC-2) Application Partitioning; (SC-3) Security Function Isolation; (SC-4) Information in Shared Resources; (SC-5) Denial of Service Protection; (SC-6) Resource Availability; (SC-7) Boundary Protection; (SC-8) Transmission Confidentiality and Integrity; (SC-9) Transmission Confidentiality; (SC-10) Network Disconnect; (SC-11) Trusted Path; (SC-12) Cryptographic Key Establishment and Management; (SC-13) Cryptographic Protections; (SC-14) Public Access Protections; (SC-15) Collaborative Computing Devices; (SC-16) Transmission of Security Attributes; (SC-17) Public Key Infrastructure Certificates; (SC-18) Mobile Code; (SC-19) Voice Over Internet Protocol; (SC-20) Secure Name / Address Resolution Service (Authoritative Source); (SC-21) Secure Name / Address Resolution Service (Recursive or Caching Resolver); (SC-22) Architecture and Provisioning for Name Address Resolution Service; (SC-23) Session Authenticity; (SC-24) Fail in Known State; (SC-25) Thin Nodes; (SC-26) Honeypots; (SC-27) Platform-Independent Applications; (SC-28) Protection of Information at Rest; (SC-29) Heterogeneity; (SC-30) Concealment and Misdirection; (SC-31) Covert Channel Analysis; (SC-32) Information System Partitioning; (SC-33) Transmission Preparation Integrity; (SC-34) Non-Modifiable Executable Programs; (SC-35) Honey-clients; (SC-36) Distributed Processing and Storage; (SC-37) Out-of-Band Channels; (SC-38) Operations Security; (SC-39) Process Isolation; (SC-40) Wireless Link Protection; (SC-41) Port and I/O Device Access; (SC-42) Sensor Capability and Data; (SC-43) Usage Restrictions; and (SC-44) Detonation Chambers.
- **System and Information Integrity (SI):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of (SI-1) System and Information Integrity Policy and Procedures; (SI-2) Flaw Remediation; (SI-3) Malicious Code Protection; (SI-4) Information System Monitoring; (SI-5) Security Alerts, Advisories, and Directives; (SI-6) Security Functions Verification; (SI-7) Software, Firmware and Information Integrity; (SI-8) SPAM Protection; (SI-9) Information Input Validation; (SI-10) Information Input Validation; (SI-11) Error Handling; (SI-12) Information Handling and Retention; (SI-13) Predictable Failure Prevention; (SI-14) Non-Persistence; (SI-15) Information Output Filtering; (SI-16) Memory Protection; and (SI-17) Fail-Safe Procedures.

- **Program Management (PM):** NCUA leverages this control family to address the establishment of policy, procedures, and practices for the effective implementation and operations of the (PM-1) Information Security Program Plan; (PM-2) Senior Information Security Officer; (PM-3) Information Security Resources; (PM-4) Plan of Action and Milestone Process; (PM-5) Information System Inventory; (PM-6) Information Security Measures of Performance; (PM-7) Enterprise Architecture; (PM-8) Critical Infrastructure Plan; (PM-9) Risk Management Strategy; (PM-10) Security Authorization Process; (PM-11) Mission/Business Process Definition; (PM-12) Insider Threat Program; (PM-13) Information Security Workforce; (PM-14) Testing, Training and Monitoring; (PM-15) Contacts with Security Groups and Associations; and (PM-16) Threats Awareness Program.

These managerial, operational, and technical controls are leveraged according to system categorization and comply with industry controls such as the GLBA the Dodd-Frank Wall Street Reform and Consumer Protection Act, the Sarbanes-Oxley Act, and the Payment Card Industry Data Security Standards.

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 at least annual 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, allowing for seamless reporting to the Department of Homeland Security's Cybersecurity and Infrastructure Security Agency (CISA).

Activities to Ensure Effective Information Technology Security

Appointment of Qualified Staff

With respect to examination staff, all examiners are trained on information technology security as part of new examiner and core examiner training. All examiners also receive periodic update training on information technology security. The NCUA also has a cadre of examiners specially trained on information technology security and other field staff positions that specialize in examining for information technology security. These subject matter experts have the technical knowledge and skills necessary to perform in-depth information technology examination work. The NCUA also has highly specialized personnel in the Office of Examination and Insurance to develop and maintain examination policies and tools, supervisory guidance, and examiner training, and coordinate with other supervisory agencies.

The NCUA has established an Enterprise Risk Management Council, a Cybersecurity Steering Council, and an Information Technology Prioritization Council comprised of senior executives with diverse backgrounds, including information technology. These councils monitor, measure, manage, and prioritize risks and related investments, including information technology 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 Officer, and the Senior Agency Officer for Privacy work closely together to ensure compliance and drive security performance. Information Systems Security Officer positions were added to certain business units in 2019 to provide specialized expertise to the NCUA offices involved in operating internal information systems to enhance the security of these systems.

The NCUA also recently created a working group to the lead the agency effort to advance toward Zero Trust Architecture, accelerate movement to secure cloud services, including Software as a Service (SaaS), Infrastructure as a Service (IaaS), and Platform as a Service (PaaS), and centralize and streamline access to cybersecurity data to drive analytics for identifying and managing cybersecurity risks. As part of this initiative, the NCUA is carefully evaluating the need for additional investment in both technology and personnel to achieve these goals.

Staff Training

The NCUA provides mandatory privacy and security awareness training to all NCUA staff. 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 is 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.
- Destroying or returning all other non-public sensitive or personally identifiable information at the conclusion of the examination or review.

Staff that have elevated access to systems or have management responsibility for systems and data are given mandatory role-based training. For the NCUA staff in cybersecurity roles, individual development plans are developed collaboratively with managers to ensure there are domain-specific skills building opportunities with at least 80 hours of instructor-led training or conferences allocated for each person. All agency staff are provided at least annually with general and role-based training on information security and cybersecurity, including their legal, reputational, and ethical obligations to protect sensitive information.

The NCUA's information technology examination training program includes classroom, online, and on-the-job training. The program is designed to specifically address competencies in the areas of information technology, 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 information technology risks. Examiners are provided training to maintain knowledge of standards, tools, and practices to identify, detect, prevent, and mitigate information technology and cybersecurity risks, threats, and vulnerabilities.

The information technology training curriculum includes courses providing instruction and practice exercises for examiners focusing on information technology concepts during examinations. The courses are designed to introduce information technology examination procedures and expand understanding of cybersecurity concepts found in the FFIEC IT Booklets, the NIST cybersecurity standards, and other recognized authoritative sources. In addition, examiners participate in on-the-job training and complete intermediate reviews under the guidance of an experienced specialized examiner.

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

Examiners are provided performance standards that are measured annually during the appraisal process. During this process, management provides feedback on performance and recommendations for improvement as appropriate.

The NCUA also conducts quality control reviews to evaluate whether an examination or report meets national standards, provide a written assessment of the report, and assess the adequacy of ongoing supervision. In addition, credit unions supervised by the Office of National Examinations and Supervision receive a pre-delivery quality control and post-delivery quality assurance review conducted by the Office of Examination and Insurance.

Credit Union Training and Support

The NCUA also provides training for credit unions. For example, the NCUA's Office of Credit Union Resources and Expansion hosted a webinar entitled Critical Security Controls and Cyber Hygiene in May 2021. This webinar provided credit unions with important information about protecting their organizations and their members from cyberattacks.

NCUA also provides credit unions resources through the NCUA website and by providing technical assistance grants and low-interest loans to low-income credit unions. Below are some other examples of resources for credit unions the NCUA provides:

- MERIT: The Modern Examination and Risk Identification Tool, otherwise known as MERIT, is the NCUA's new examination tool replacing AIRES, a legacy examination platform. MERIT offers credit unions enhanced ability to securely transfer files within the context of an examination, provide status updates and request due date changes on examination findings and action items, and retrieve completed examination reports.
- ACET Application: The NCUA developed an application for credit unions that houses the ACET. The cybersecurity maturity assessment module in the application guides credit unions through the process of completing an ACET. It 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 provides the credit union with a measure a level or risk and corresponding controls.
- NCUA Website: The NCUA website provides additional cybersecurity resources for research and informational purposes. The Cybersecurity Resources page, in particular, 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 union growth through the Community Development Revolving Loan Fund (CDRLF). In 2019, the NCUA awarded more than $2.0 million in technical assistance and urgent needs grants to 166 low-income designated credit unions. Recipients used these funds to increase their digital services and improve their levels of

cybersecurity preparedness, engage in leadership and career development, and improve access to financial services. The agency has renewed its CDRLF cybersecurity grants in 2021, and the Chairman recently requested that the Congress consider appropriating $10 million for CDRLF to further the reach of these vital funds throughout the credit union system. Increased CDRLF funding would allow the agency to make more grants and at larger amounts. Every penny appropriated for CDRLF goes to credit unions and no appropriated funds are used for the administration of the program.

Agency Investment in Information Technology Security

The NCUA has invested funds in the area of network and security infrastructure and added staff focused on cybersecurity and privacy. 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. Among the resources added were cyber-incident responders, risk and compliance specialists, and network security engineers. The agency also hired individuals with specialized skills using contracted staff to mitigate the organizational skills gap in the areas of computer forensics, defensive cyber operations, malware analysis and mitigation, security information and event management, configuration and management, threat hunting, and incident handling and response.

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 tunnels and internal and external network traffic is managed and monitored.

To enhance visibility into network and infrastructure operations and observable anomalous behaviors, NCUA procured, implemented, and optimized a security information and event management solution. NCUA also leverages Department of Homeland Security’s EINSTEIN infrastructure to enhance cybersecurity analysis, situational awareness, and security response in Internet traffic and connections.

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, 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, 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, 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, NCUA migrated to Microsoft's Office 365 environment with a projected completion of all services migrated by CY 2023.

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.

Audits and Reviews of NCUA's Information Technology Security Efforts

The NCUA's OIG conducts independent audits, investigations, and other activities to verify 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. These notices are the subject of Plans of Action and Milestones and are systematically remediated over time. NCUA has been graded as "Managing Risk."

In addition, as indicated in the Financial Statement Audits, the NCUA complies with the requirements of the Federal Managers' Financial Integrity Act of 1982. 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.

The OIG has made three recommendations to the NCUA following three recent audits. The NCUA concurred with the results of the audits and responded to the OIG recommendations. A summary of each audit is provided below:

- Audit of the NCUA Information Technology Examination Program's Oversight of Credit Union Cybersecurity Programs
  - **Objective:** In September 2017, the NCUA OIG conducted a self-initiated audit to assess NCUA's IT examination program. The objective was to determine whether the IT examination program provides for adequate oversight of federally insured credit union cybersecurity programs and to assess whether credit unions were taking sufficient and appropriate measures to protect the confidentiality, availability, and

integrity of credit union assets and sensitive credit union information against cyberattacks.

- **Recommendation:** As a result of the audit, the OIG recommended that the NCUA adapt its IT examination program to incorporate the ACET, NCUA's risk-focused examination program, to ensure more comprehensive examinations of credit unions' cybersecurity programs. The NCUA concurred with the OIG recommendation to incorporate the ACET into its risk-focused examination program.
- **Action:** By year-end 2018, NCUA conducted ACET reviews in 86 percent of credit unions greater than $1 billion in assets. By year-end 2019, NCUA completed ACET reviews on 100 percent of credit unions with assets greater than $1 billion, and 43 percent of credit unions with between $250 million and $1 billion in assets.
    - Due to the COVID-19 pandemic, the agency's Supervisory Priorities were updated in July 2020, resulting in a transition from performing ACET maturity assessments to piloting the InTREx-CU.

- Audit of the NCUA Office of National Examinations and Supervision (ONES) Oversight of Credit Union Cybersecurity Programs
    - **Objective:** In 2019, the NCUA OIG conducted a self-initiated audit to further assess NCUA's IT examination program. The objective of the audit was to determine whether the NCUA's Office of National Examinations and Supervision provided adequate oversight of its credit unions' cybersecurity programs and to assess whether the credit unions were taking sufficient and appropriate measures to protect the confidentiality, availability, and integrity of credit union assets and sensitive credit union data against cyberattacks.
    - **Recommendation:** The audit determined that the Office of National Examinations and Supervision provided adequate oversight of its credit unions' cybersecurity programs. As a result, the OIG did not make any additional recommendations.
- Audit of the NCUA's Examination and Oversight Authority Over Credit Union Service Organizations and Vendors
    - **Objective:** In 2020, the NCUA OIG conducted this self-initiated audit to assess the NCUA's examination and oversight authority of CUSOs and third-party vendors. The objectives of the audit were to determine whether:
        1) The NCUA complied with applicable laws, regulations, policies, and procedures for CUSO and other non-CUSO third-party vendor reviews; and
        2) The NCUA's vendor review process effectively helps to assess the adequacy of credit union management's due diligence reviews and identify and reduce the risks vendor relationships pose to credit unions.

- **Recommendation:** Results of the audit determined that the NCUA complied with applicable laws, regulations, policies, and procedures for CUSO reviews. The OIG also determined that the NCUA's authority regarding CUSOs and vendors is limited and that statutory authority over CUSOs and vendors could enable the agency to more effectively identify and reduce the risks that CUSOs and vendors pose to credit unions. This is of particular concern in light of credit unions' increased reliance on CUSOs and vendors to perform mission-critical functions, including technology services, which impact over 120 million credit union members.
- **Action:** NCUA concurred with the recommendation and indicated that post recovery the agency plans to work with Congress on providing the NCUA vendor authority to allow the agency to better supervise for third-party cybersecurity risks. NCUA also added to its response that for the past two decades NCUA has requested Congress reinstate the vendor authority similar to that of the other federal banking regulators. The agency originally received temporary vendor authority through the Examination Parity and Year 2000 Readiness for Financial Institutions Acts. This temporary vendor authority was discontinued in December 2001 when the Act sunset. Since that time, multiple NCUA leaders have signaled support for the reinstatement of vendor authority in congressional testimonies and letters.

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 made significant improvements to their IT programs. Over the last four years, IT risk factors requiring immediate attention, issued to credit unions in the form of documents of resolution, have significantly decreased.

The credit union system has responded positively to the efforts of the financial regulators by incorporating regulator's 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. Treasury Department-led Hamilton Series Exercises to develop one-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 due to a catastrophic event.

Coordination Efforts

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

FFIEC Council: 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. The NCUA is the current chair of the FFIEC and has representation on all task forces of the FFIEC.

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 member agencies that supervise banks, thrifts, and credit unions 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:** The Information Technology Subcommittee serves as a forum to address 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 serves as a forum to address policy relating to cybersecurity and critical infrastructure security and 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 Risks, 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 ten voting members and five 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 Department of Treasury and chartered under the President's Working Group on Financial Markets, which was established by Executive Order 12631. Working with appropriate members of financial regulatory agencies, 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 2020, the NCUA and Treasury held an exercise simulating a ransomware attack specifically for credit unions.

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 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.

Current and Emerging Threats

The NCUA remains concerned about the risks that cyberattacks pose to the financial system. To compete, credit unions must be able to safely and securely use technology to deliver member services and adopt financial innovation to ensure the industry's long-term success. The likelihood of these threats adversely affecting credit unions and their consumers continues to rise in correlation to the advances and adoption of financial technology. More specifically, current and emerging cybersecurity threats to credit unions include:

Ransomware: Ransomware is the most immediate threat to critical infrastructures, with the integration of data theft extortion to many ransomware operations accounting for a significant increase posed by these 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 and deliver mission critical services. To increase pressure on organizations to pay extortion demands, cyber intruders have evolved their tactics to 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 any financial institution to defend against such attacks.

Supply Chain/Third-Party Vendors: Cyber actors continue to focus their efforts on exploiting vulnerabilities identified across U.S. infrastructure sectors and systems, including those of third-party providers of IT services. 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 service providers and cloud service providers, has drastically increased in recent years because IT service providers enable credit unions to more cost effectively scale and support network environments. By servicing numerous customers, IT service providers can achieve significant economies of scale. However, outsourcing processes or functions does not eliminate credit union responsibility for the safety and soundness of those processes and functions.

Credit unions should know that the decision to centralize information with an IT service provider could present risks to the confidentiality and integrity of their information. For example, IT service providers generally have direct access to credit union networks and may store member data on their own internal infrastructure. A compromise, therefore, in one part of an IT service provider's network can have cascading effects, affecting credit unions and introducing systemic risk.

NCUA's Lack of Vendor Authority: Currently, the NCUA may only examine CUSOs and third-party vendors with their permission, and vendors, at times, decline these requests. Further, vendors can reject the NCUA's recommendations to implement appropriate corrective actions to mitigate identified risks. For example, in the past, several vendors refused to implement the NCUA's recommendations to improve network security and safeguard sensitive member information due to cost concerns. This stands in stark contrast to the authority of the NCUA's counterparts on the FFIEC.

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 outside of NCUA's regulatory oversight. In addition, credit unions are increasingly using third-party vendors to provide technological services, including information security and mobile and online banking. Member data are also being stored on vendors' servers. The pandemic, which has accelerated the industry's movement to digital services, has only increased credit union reliance on third-party vendors.

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

The continued transfer of operations to CUSOs and other third parties diminishes the ability of the NCUA 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 Financial Stability Oversight Council, 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, have also requested legislative action to provide vendor authority.

Conclusion

The NCUA continues to promote safe and sound cybersecurity 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 in 2020, 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 2021 grant initiative, the agency is again funding cybersecurity grants. The NCUA is also strengthening cybersecurity reviews during regular examinations of credit unions and will move to fully implement the InTREx-CU in 2022.

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

Appendix: Resources

Laws, Regulations, and Reporting

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)	

NCUA Letters to Credit Unions

Year:	Letter:	Letters to Credit Unions:
2017	17-CU-08	Interagency Supervisory Guidance for Institutions Affected by a Major Disaster
2016	16-CU-12	Risk-Based Examination Scheduling Policy
2011	11-CU-09	Online Member Authentication Guidance Compliance Required by January 2012
2011	11-CU-13	Emergency Financial Services for Disaster Victims
2007	07-CU-13	Evaluating Third Party Relationships
2006	06-CU-13	Authentication for Internet Based Services

Year:	Letter:	Letters to Credit Unions:
2006	06-CU-10	NCUAs Information System and Technology IST Program
2006	06-CU-07	IT Security Compliance Guide for Credit Unions
2005	05-CU-18	Guidance on Authentication in Internet Banking Environment
2004	04-CU-14	Risk Management of Free and Open Source Software
2003	03-CU-08	Web linking Identifying Risks Risk Management Techniques
2003	03-CU-14	Computer Software Patch Management
2003	03-CU-07	FFIEC Release of Information Technology Examination Handbook
2003	03-CU-03	Wireless Technology
2002	02-CU-17	e-Commerce Guide for Credit Unions
2002	02-CU-08	Account Aggregation Services
2002	02-CU-16	Protection of Credit Union Internet Addresses
2002	02-CU-13	Vendor Information Systems Technology Reviews Summary Results
2001	01-CU-12	e-Commerce Insurance Considerations
2001	01-CU-10	Authentication in an Electronic Banking Environment
2001	01-CU-11	Electronic Data Security Overview
2001	01-CU-04	Integrating Financial Services and Emerging Technology
2001	01-CU-20	Due Diligence Over Third Party Service Providers
2000	00-CU-07	NCUAs Information Systems Technology Examination Program
2000	00-CU-11	Risk Management of Outsourced Technology Services
1997	97-CU-05	Interagency Statement on Retail On-line PC Banking
1991	91-CU-122	NCUA Reviews of EDP Vendors
1989	89-CU-109	Information Processing Issues
1989	08-CU-09	Evaluating Third Party Relationships Questionnaire

NCUA Risk Alerts

Year:	Reference:	Alert:
2020	20-RISK-02	Cybersecurity Considerations for Remote Work
2019	19-RISK-01	Business Email Compromise Fraud
2013	13-RISK-01	Mitigating Distributed Denial-of-Service Attacks
2011	11-RISK-01	Security Breach involving RSA SecurID Tokens
2009	09-RISK-01	Information Systems & Technology
2006	06-RISK-01	Disaster Planning and Response
2005	05-RISK-01	Raising Consumer Awareness of Phishing Schemes

NCUA Supervision Priorities

Year:	Letter:	Reference:
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 Supervisory Policy Manual (NSPM)

Reference:	Resource:
Examiner’s Guide	COVID-19
Examiner’s Guide	Risk-Focused Examinations
NSPM	NSPM Public v14.0

NCUA Joint Statement Cybersecurity Press Releases

Date:	Press Release:
3/29/2021	Agencies Seek Wide Range of Views on Financial Institutions’ Use of Artificial Intelligence
2/22/2021	Federal and State Regulatory Agencies Issue Examiner Guidance for Assessing Safety and Soundness Considering the Effect of the COVID-19 Pandemic on Financial Institutions
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

NCUA Cybersecurity Resources Web Page

Resource:
Examiner’s Guide
AIRES IT Questionnaires
FFIEC Cybersecurity Assessment Tool Frequently Asked Questions
FFIEC Cybersecurity Assessment Tool
NIST Special Publications
Security and Privacy Controls for Federal Information Systems and Organizations

Resource:
Financial Services Information Sharing and Analysis Center
National Credit Union Information Sharing Analysis Organization
FFIEC Cybersecurity Assessment General Observations
Cybersecurity Threat and Vulnerability Monitoring and Sharing Statement
FBI Infragard
Federal Financial Institutions Examination Council (FFIEC) IT Examination Handbook Infobase
Twenty Critical Security Controls for Effective Cyber Defense
SANS Reading Room Best Practices
Technical Guide to Information Security Testing and Assessment
Federal CIO Council Privacy Committee, Best Practices: Elements of a Federal Privacy Program Version 1.0
Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)
Security and Privacy Controls for Federal Information Systems and Organizations (Appendix J)
FAQs on Ransomware and Supply Chain Risk Management
Ransomware Information
Payment Card Industry (PCI)
Federal Reserve Financial Services – Federal Reserve Bank Operating Circulars
FFIEC Bank Secrecy Act / Anti-Money Laundering Examination Manual
NACHA Operating Rules
Uniform Commercial Code Article 4A

FFIEC IT Booklets

Release Date:	Reference:	Booklet:
6/2021	FFIEC IT Booklet	Architecture, Infrastructure, and Operations

Release Date:	Reference:	Booklet:
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
8/2003	FFIEC IT Booklet	E-Banking

FFIEC Cybersecurity Awareness: Resources

Resource:
FFIEC Statement on Security in a Cloud Computing Environment
FFIEC Office of Foreign Assets Control Cyber-Related Sanctions Program Risk Management
FFIEC Cybersecurity Resource Guide for Financial Institutions
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
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
10/6/2016	The Federal Financial Institutions Examination Council (FFIEC) Announces Webinars in Observance of Cybersecurity Awareness Month
6/7/2016	FFIEC Issues Statement on Safeguarding the Cybersecurity of Interbank Messaging and Payment Networks
11/3/2015	FFIEC Releases Statement on Cyber Attacks Involving Extortion
6/30/2015	FFIEC Releases Cybersecurity Assessment Tool
3/30/2015	FFIEC Releases Two Statements on Compromised Credentials and Destructive Malware
3/17/2015	FFIEC Focuses on Cybersecurity, Will Debut Self-Assessment Tool
11/3/2014	FFIEC Releases Cybersecurity Assessment Observations, Recommends Participation in Financial Services Information Sharing and Analysis Center
9/26/2014	State and Federal Regulators: Financial Institutions Should Move Quickly to Address Shellshock Vulnerability
6/24/2014	FFIEC Launches Cybersecurity Web Page, Promotes Awareness of Cybersecurity Activities
5/7/2014	FFIEC Promotes Cybersecurity Preparedness for Community Financial Institutions
4/10/2014	Financial Regulators Expect Firms to Address OpenSSL "Heartbleed" Vulnerability

Date:	Statements:
4/2/2014	Financial Regulators Release Statements on Cyber-Attacks on Automated Teller Machine and Card Authorization Systems and Distributed Denial of Service Attacks
10/7/2013	Press Release: Financial Regulators Release Statement on End of Microsoft Support for Windows XP Operating System
10/2/2013	FFIEC Supports National Cybersecurity Awareness Month