



---

National Credit Union Administration  
Office of External Affairs and Communications

---

June 23, 2025

SENT BY EMAIL

The Honorable Tim Scott  
Chairman  
U.S. Senate Committee on Banking, Housing, and Urban Affairs  
534 Dirksen Senate Office Building  
Washington, DC 20510

Dear Mr. Chairman:

Enclosed please find the NCUA's 2025 *Cybersecurity and Credit Union System Resilience Report to Congress*, submitted in compliance with Section 108 of the Consolidated Appropriations Act, 2021, P.L. 116-260. This report summarizes the agency's efforts to strengthen cybersecurity within the financial services sector with respect to the agency's function as a regulator, including its supervision of federally insured credit unions.

If you have questions about the agency's submission, please feel free to contact me at 703-215-7784 or [oeacmail@ncua.gov](mailto:oeacmail@ncua.gov).

Sincerely,

A handwritten signature in black ink that reads "Sierra Robinson".

Sierra Robinson  
Director

Enclosure



---

National Credit Union Administration  
Office of External Affairs and Communications

---

June 23, 2025

SENT BY EMAIL

The Honorable Maxine Waters  
Ranking Member  
U.S. House Committee on Financial Services  
4340 O'Neill House Office Building  
Washington, DC 20515

Dear Ranking Member Waters:

Enclosed please find the NCUA's 2025 *Cybersecurity and Credit Union System Resilience Report to Congress*, submitted in compliance with Section 108 of the Consolidated Appropriations Act, 2021, P.L. 116-260. This report summarizes the agency's efforts to strengthen cybersecurity within the financial services sector with respect to the agency's function as a regulator, including its supervision of federally insured credit unions.

If you have questions about the agency's submission, please feel free to contact me at 703-215-7784 or [oeacmail@ncua.gov](mailto:oeacmail@ncua.gov).

Sincerely,

A handwritten signature in black ink that reads "Sierra Robinson".

Sierra Robinson  
Director

Enclosure



---

National Credit Union Administration  
Office of External Affairs and Communications

---

June 23, 2025

SENT BY EMAIL

The Honorable French Hill  
Chairman  
U.S. House Committee on Financial Services  
2129 Rayburn House Office Building  
Washington, DC 20515

Dear Mr. Chairman:

Enclosed please find the NCUA's 2025 *Cybersecurity and Credit Union System Resilience Report to Congress*, submitted in compliance with Section 108 of the Consolidated Appropriations Act, 2021, P.L. 116-260. This report summarizes the agency's efforts to strengthen cybersecurity within the financial services sector with respect to the agency's function as a regulator, including its supervision of federally insured credit unions.

If you have questions about the agency's submission, please feel free to contact me at 703-215-7784 or [oeacmail@ncua.gov](mailto:oeacmail@ncua.gov).

Sincerely,

A handwritten signature in black ink that reads "Sierra Robinson".

Sierra Robinson  
Director

Enclosure



---

National Credit Union Administration  
Office of External Affairs and Communications

---

June 23, 2025

SENT BY EMAIL

The Honorable Elizabeth Warren  
Ranking Member  
U.S. Senate Committee on Banking, Housing, and Urban Affairs  
534 Dirksen Senate Office Building  
Washington, DC 20510

Dear Ranking Member Warren:

Enclosed please find the NCUA's 2025 *Cybersecurity and Credit Union System Resilience Report to Congress*, submitted in compliance with Section 108 of the Consolidated Appropriations Act, 2021, P.L. 116-260. This report summarizes the agency's efforts to strengthen cybersecurity within the financial services sector with respect to the agency's function as a regulator, including its supervision of federally insured credit unions.

If you have questions about the agency's submission, please feel free to contact me at 703-215-7784 or [oeacmail@ncua.gov](mailto:oeacmail@ncua.gov).

Sincerely,

A handwritten signature in cursive script that reads "Sierra Robinson".

Sierra Robinson  
Director

Enclosure

# Cybersecurity and Credit Union System Resilience Report

June 2025

National Credit Union Administration  
Alexandria, VA



## TABLE OF CONTENTS

<b>Introduction</b> .....	<b>2</b>
<b>1. Analysis of Policies and Procedures</b> .....	<b>3</b>
Policies and Procedures .....	3
Regulations.....	4
Examination and Supervision Program.....	4
<b>2. Activities to Ensure Effective Implementation of Policies and Procedures</b> .....	<b>6</b>
Qualified Staff.....	6
Deployment of Adequate Resources and Technologies.....	8
Office of the Inspector General.....	8
Industry Efforts.....	9
Interagency Coordination to Strengthen Cybersecurity.....	9
<b>3. Current and Emerging Threats</b> .....	<b>11</b>
<b>Conclusion</b> .....	<b>12</b>
<b>Appendix: Resources</b> .....	<b>13</b>
Regulations.....	13
Letters to Credit Unions .....	13

## INTRODUCTION

The Cybersecurity and Credit Union System Resilience Report details the measures taken to strengthen cybersecurity within credit unions and the National Credit Union Administration (NCUA), as required by the [Consolidated Appropriations Act, 2021 \(P.L. 116-260\)](#).<sup>1</sup> This report:

- Outlines the NCUA's policies and procedures to address cybersecurity risks and activities;
- Discusses cybersecurity resilience within the credit union system, including the NCUA's key initiatives to enhance cybersecurity preparedness among credit unions, such as targeted examinations, risk assessments, and educational and outreach efforts;
- Describes current and emerging threats; and
- Highlights the NCUA's collaboration with other federal agencies, industry stakeholders, and cybersecurity experts to address emerging threats and promote a culture of cybersecurity awareness and resilience within the credit union industry.

The report underscores the NCUA's ongoing commitment to protecting the financial well-being of credit union members and upholding the integrity of the broader financial system in the face of cybersecurity threats.

Credit unions are an essential provider of financial services to the American public, with transaction activity that exceeded \$86 trillion in 2024.<sup>2</sup> Together, credit unions and the NCUA remain vigilant to the ever-present threat of cyberattacks.

---

<sup>1</sup> Pub. L. No. 116-260, 134 Stat. 2173 (Dec. 27, 2020)

<sup>2</sup> Source: [Nacha.org](https://www.nacha.org)

## 1. ANALYSIS OF POLICIES AND PROCEDURES

The NCUA policies and procedures, regulations, and the examination and supervision program together demonstrate how the NCUA detects, defends, and responds to cybersecurity threats and other efforts that may threaten the NCUA or federally insured credit unions.

### Policies and Procedures

#### **Agency Cybersecurity Program**

The NCUA has minimal tolerance for IT system risk.<sup>3</sup> The agency complies with mandatory security standards for federal information and information systems and must meet minimum information security requirements by using security and privacy controls recommended by the National Institute of Standards & Technology (NIST) and the Federal Information Security Modernization Act of 2014 (FISMA).<sup>4,5</sup>

The NCUA implements applicable statutes, regulations, and standards including the NIST Risk Management Framework and Special Publication 800-53 – *Security and Privacy Controls for Information Systems and Organizations*.<sup>6</sup> The agency also complies with the Cybersecurity and Infrastructure Agency’s (CISA’s) binding operational, emergency and cybersecurity coordination, assessment, and response directives.

The NCUA is actively adopting a zero-trust security model based on the principle of maintaining strict access controls. As part of system authorization, the NCUA considers:

- Information types, assets, and systems;
- Identity verification and access enforcement;
- Device health and posture;
- Roles and privileges of those who manage and operate the systems;
- Interconnections of systems and data; and
- Privacy Impact Assessments, Privacy Plans, and Systems of Records Notices.

<sup>3</sup> NCUA Risk Appetite Statement (October 20, 2022). The risk appetite for technology and information management for operational IT and IT systems is “averse.”

<sup>4</sup> 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.

<sup>5</sup> NIST Special Publication 800-53, Security and Privacy Controls for Federal Information Systems and Organizations.

<sup>6</sup> NCUA is also subject to federal statutes including FISMA, 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.

Based on information and system sensitivity, the NCUA selects and implements the security controls necessary to protect the confidentiality, integrity, and availability of the organizational systems and critical infrastructure. The security controls are documented, reviewed, and tested to verify they produce the desired outcome.

Once authorized, systems are continuously monitored using automated and manual processes with regular testing of controls to validate their continued efficacy.

The NCUA also strengthens information security by designing and disseminating fully developed agency-wide and program-specific policies and procedures to establish appropriate practices for collecting, encrypting, 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, CISA, or the National Archives and Records Administration.

## Regulations

### **Information Security and Cybersecurity Regulations**

Pursuant to the [Gramm-Leach-Bliley Act](#) (P.L. 106-102), the NCUA established standards for federally insured credit unions relating to administrative, technical, and physical safeguards for credit union member records and information. These standards are incorporated into the NCUA's regulations at 12 Code of Federal Regulations (C.F.R.) part 748, Appendix A, [Guidelines for Safeguarding Member Information](#).

In February 2023, the NCUA Board approved a [final rule](#) requiring federally insured credit unions to notify NCUA no later than 72 hours after a credit union reasonably believes a reportable cyber incident occurred.

The Cyber Incident Notification Rule provides the NCUA with an early notification system so the NCUA may detect and respond to cyber incidents that may be systemic in the credit union system or the broader financial services sector. For those incidents, the NCUA would initiate the interagency protocols for incident response. From May 1, 2024, through April 30, 2025, credit unions reported 539 cyber incidents related to ATM jackpotting, business email compromises and phishing attacks, ransomware, and third-party service providers. No incident reported during this period was systemic to the credit union system.

## Examination and Supervision Program

### **Information Security Examination Program**

The NCUA's Information Security Examination (ISE) program assesses cybersecurity resilience within the credit union system. The ISE program evaluates a credit union's preparedness for malicious cyberattacks and credit unions use examination feedback to strengthen their programs and protect their members.

At each examination, the NCUA performs an information security review using the ISE program, which uses a risk-focused, scalable approach to examine a credit union's

information security program. This provides examiners the flexibility to focus on areas of current or potential material risk relevant to each credit union's unique business model. ISE program objectives 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 systems and technology operations;
- Assessing the adequacy of internal information systems and technology controls and oversight to safeguard member information; and
- Determining whether the credit union's Board of Directors is providing adequate governance over information systems and security.

The ISE program focuses on NCUA regulations 12 C.F.R. parts 748, [Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance](#), and 749, [Records Preservation Program and Appendices – Record Retention Guidelines, Catastrophic Act Preparedness Guidelines](#).

The ISE procedures reference industry security standards and frameworks from NIST and the Center for Internet Security, and CISA.

### **Automated Cybersecurity Evaluation Toolbox (ACET) Maturity Assessment**

The ACET maturity assessment is a tool provided and maintained by the NCUA for voluntary credit union use. Credit unions may use the ACET to determine the maturity of their information security programs. Aligned with NCUA's ISE program, the ACET incorporates appropriate cybersecurity standards and practices established for financial institutions and maps declarative statements to applicable elements of the [FFIEC IT Examination Handbook](#), regulations, and industry standards like the NIST Cybersecurity Framework.

### **Information Technology & Cybersecurity Alerts**

Between July 2024 and May 2025, the NCUA issued the following cybersecurity alerts and notices to help federally insured credit unions remain aware of common vulnerabilities and exposures (CVEs):

- **ATM Skimming Activity Reported in the North Canton Area of Ohio** – After receiving reports of ATM skimming devices in a specific area, the NCUA issued an alert for nearby ATM owners. (7/25/24)
- **Board of Directors Engagement in Cybersecurity Oversight Letter to Credit Unions** – The NCUA issued this letter to credit unions after a ransomware attack on a credit union was attributed to “malvertising,” a relatively new cyberattack technique that injects malicious code within digital ads. The NCUA recommended credit union Boards of Directors engage in ongoing education about current cybersecurity threats, trends, and best practices. (10/21/2024)

- **CISA Critical FortiManager Vulnerability (CVE-2024-47575)**— After CISA issued an alert addressing a critical FortiManager vulnerability, the NCUA followed suit encouraging credit unions reliant on Fortinet technology to review the guidance for CVE-2024-47575 and take any necessary steps. (11/7/24)
- **CISA February and March 2025 Vulnerability Scanning**— The NCUA issued a cybersecurity alert summarizing CISA’s vulnerability snapshot for the financial services sector. The NCUA cybersecurity alert outlined vulnerabilities and provided details and links for more information on known CVEs. (5/7/25)

## 2. ACTIVITIES TO ENSURE EFFECTIVE IMPLEMENTATION OF POLICIES AND PROCEDURES

### Qualified Staff

The NCUA employs highly qualified staff who focus on cybersecurity and privacy. IT security staff include cybersecurity operations and incident responders, cloud security architects, application security architects, 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;
- Malware analysis and mitigation;
- Security information and event management;
- Configuration management;
- Threat hunting;
- Security awareness and education;
- Governance, risk, and compliance; and
- Incident handling and response.

### **Training**

#### For NCUA Staff

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. All agency employees and contractors receive general and role-based training on information security and cybersecurity at least annually. This training addresses individual employees’ legal, reputational, and ethical obligations to protect sensitive information. Staff are trained on:

- Collecting information in a secure manner using a hierarchy of secure methods that best suit the situation;
- Transferring and storing sensitive information where there is an identified and authorized need, and in a manner consistent with agency instructions; and
- Destroying or returning all other non-public sensitive or personally identifiable information after the examination or review, per applicable laws.

**Privileged Access**— Staff with privileged access to systems, or who manage systems and data, take mandatory role-based training.

**Credit Union Examiners**— The NCUA provides training for examiners specific to the ISE program. Examiners gain knowledge on standards, tools, and practices to identify, detect, prevent, and mitigate IT and cybersecurity risks, threats, and vulnerabilities.

**Specialized Examiners**— NCUA's regional and national IT Security examiners receive specialized training to develop and maintain technical knowledge and skills required to perform in-depth information security examinations at more complex institutions.

#### Credit Union Training and Support

The NCUA's Office of Credit Union Resources and Expansion provides training for credit unions. The NCUA maintains an online system with more than 300 courses on various topics, including information security, which is available to credit unions at no cost. The office also hosts webinars to deliver timely and meaningful information to help credit union professionals stay current on relevant topics affecting the credit union community. These webinars provide important information on how to protect credit unions and members.

#### **Accountability Measures and Senior Leadership**

The NCUA's Enterprise Risk Management Council, Cybersecurity Council, and IT Oversight Council are each comprised of senior executives with diverse backgrounds, including information technology and security. Together, these three bodies provide accountability and strengthen oversight of the agency cybersecurity program. The Office of Examination and Insurance in concert with the NCUA regions and other internal offices implement the supervision and examination program of credit unions. The agency's [2025 Annual Performance Plan](#) outlines the NCUA's resources and strategies the NCUA setting priorities and managing performance.

#### Federal Managers' Financial Integrity Act

The Federal Managers' Financial Integrity Act (FMFIA) P.L. 97-255, establishes management's responsibility to annually assess controls and provide a Statement of Assurance to the President and Congress on the effectiveness of controls.

The NCUA continued to demonstrate our commitment to maintain a strong internal control environment. Enterprise risk management and internal controls are embedded in the

agency's management of activities and operations that achieve strategic goals and objectives. In 2024, NCUA management conducted reviews including annual internal control assessments to verify that controls effectively mitigated programmatic risks to ensure effective and efficient operations, reliable reporting, compliance with laws, and safeguarding of assets. While no material weaknesses in the agency's internal controls were identified in the assessments, the NCUA remains committed to enhancing and improving its systems of internal controls and operational efficiencies.

## Deployment of Adequate Resources and Technologies

### **2024 Annual Budget Resources**

It is the Board's responsibility to determine the resources necessary to carry out the NCUA's responsibilities under the Act. Two key objectives in the 2024 budget are ensuring robust cybersecurity in the credit union system and the NCUA and enhancing the examination and supervision program by further developing specialist examiners in areas of emerging complexity. The largest share of the agency's capital budget supports Executive Order 14028, *Improving the Nations's Cybersecurity*.

### Office of the Inspector General

The NCUA's Office of the Inspector General (OIG) conducts independent and objective audits, investigations, and other activities ensuring compliance with applicable laws, regulations, and standards. OIG audit reports, semiannual reports, and letters to Congress are available on the NCUA's website. NCUA senior leaders are briefed quarterly on the agency's progress in mitigating open findings.

### **FISMA Audit**

The NCUA conducted its fiscal year 2024 independent evaluation of the effectiveness of its information security program and practices.<sup>7</sup> The resulting audit report reflects the NCUA maintained Maturity Level 4 "Managed and Measurable." The rating reflects an effective information security program and stated the NCUA substantially complied with information security and privacy policies, and procedures.

### **Financial Statement Audit**

The OIG conducted its independent financial statement audit of the NCUA's financial statements, which included the National Credit Union Share Insurance Fund, the Operating Fund, the Central Liquidity Facility, and the Community Development Revolving Loan Fund for the years ended 2023 and 2024. The audit looks at systems, controls, and legal compliance. The result was a clean audit opinion.

---

<sup>7</sup> FISMA 2014, Public Law 113-283, requires Inspectors General to perform annual independent evaluations to determine the effectiveness of agency information security programs and practices.

## Industry Efforts

Credit union participation in the following initiatives reflects the credit union system's engagement with the broader information security community.

- **Financial Information Sharing and Analysis Centers and Organizations**— Credit unions can participate in the Financial Services Information Sharing and Analysis Center (FS-ISAC) and the National Credit Union Information Sharing and Analysis Organization (NCU-ISAO) to share intelligence, knowledge, and practices; and to collaborate and coordinate to identify, protect, detect, respond, and recover from threats and vulnerabilities.
- **Sheltered Harbor**— Comprised of financial institutions, core service providers, national trade associations, alliance partners, and solution providers dedicated to enhancing financial sector stability and resiliency, Sheltered Harbor is a subsidiary of the FS-ISAC. It assists financial institutions in preparing for catastrophic events. The standards are designed to help institutions plan for and recover from catastrophic events, and to support continuity of operations and service in a crisis.
- **CISA Cyber Hygiene Services**— More than 300 credit unions engaged with CISA's Cyber Hygiene Services program, which offers vulnerability scanning and web application scanning to help institutions mitigate cybersecurity threats.

## Interagency Coordination to Strengthen Cybersecurity

The NCUA coordinates with other federal and state regulatory agencies to strengthen cybersecurity, including developing and disseminating best practices and sharing information. Examples include the following collaborative bodies:

- **FFIEC**— In particular, the NCUA participates in the FFIEC's **Information Technology Subcommittee**. This group addresses information systems and technology policy issues as they relate to financial institutions and their technology service providers. The NCUA also participates in the **Cybersecurity Critical Infrastructure Subcommittee**. This group addresses policy and information sharing relating to cybersecurity, critical infrastructure security, and the resilience of financial institutions and technology service providers. Agency subcommittee members participate in the development of interagency and joint statements and work products. During this period, the agency collaborated with other FFIEC agencies and published the "Development, Acquisition, and Maintenance" IT Examination Handbook, part of the IT Booklet series. This booklet guides examiners in assessing information technology practices and establishes fundamental examination expectations including governance, risk management, maintenance, and change management practices.
- **Financial Stability Oversight Council (FSOC)**— The FSOC was established by Congress in the Dodd-Frank Wall Street Reform and Consumer Protection Act, P.L.

111-203 and is responsible for safeguarding the financial stability of the nation. The NCUA Chairman is actively involved in the FSOC as the agency principal and voting member. In its 2024 annual report, the FSOC recommended all financial sector participants stay updated on cybersecurity developments within the financial sector and work to reduce cybersecurity risks.

- **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. Through monthly meetings, staff from the NCUA and other FBIIC member organizations work on operational and tactical issues related to critical infrastructure matters, including cybersecurity, within the financial services industry. The U.S. Department of the Treasury’s Office of Cybersecurity and Critical Infrastructure Protection (OCCIP) works with the Financial Sector Information Sharing and Analysis Center to support development of cybersecurity exercises.
- **Financial Services Sector Coordinating Council (FSSCC)** – The NCUA collaborates and coordinates with the private sector through the FSSCC. The FSSCC collaborates with key government agencies to protect the nation’s critical infrastructure from cybersecurity and physical threats.
- **CISA** – The NCUA is part of CISA’s Vulnerability Disclosure Policy (VDP) Platform, streamlining day-to-day operations when disclosing and managing cyber vulnerabilities. The platform serves as the primary point of entry for receiving, triaging, and routing vulnerabilities discovered and reported by public security researchers in support of Binding Operational Directive 20-01: Develop and Publish a VDP.
- **OCCIP and CISA** – As a federal agency, the NCUA follows CISA and OCCIP’s joint 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 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 the following interagency initiatives:

- CISA security operations center information and collaboration sessions;
- OCCIP information and collaboration sessions;
- The Small Agency Chief Information Officer Council; and
- The Small/Micro-Agency Chief Information Security Officers Council.

### 3. CURRENT AND EMERGING THREATS

The financial sector faces an increasingly sophisticated array of cybersecurity threats that demand vigilance. The rapid evolution of technology, coupled with escalating geopolitical tensions, has expanded the threat landscape. Cybersecurity risks grow as threats evolve, become more sophisticated, and cause greater damage. Geopolitical tensions increase the possibility of nation-states and other sophisticated actors conducting malicious cyberattacks against the financial services sector, including the credit union system. Financial institutions are increasingly vulnerable due to system integration complexity, lack of service provider diversity, and vendor lock-in. The industry's long-term success depends on credit unions using appropriate cybersecurity practices and controls when delivering member services.

The evolving array of cybersecurity threats that require continued vigilance by credit unions include:

- **Artificial Intelligence (AI)-enabled Attacks**— Generative AI creates new text, images, video, and other content. Generative AI has gone mainstream and is increasingly being used by cyber actors to create complex malware and advanced social engineering attacks, including phishing and spoofing. By making these attacks more effective, they are also harder to detect and prevent. In addition to generative AI being used for initial attack vectors, it can also amplify threats once an initial breach has occurred. AI tools can be used to modify code at scale, quickly giving control to attackers. These tools can also be trained on a dataset of known vulnerabilities and used to automatically generate new exploit code to target multiple vulnerabilities in rapid succession. Cyber actors can also use generative AI to scan and summarize massive amounts of company data to identify employees, relationships, and assets, potentially leading to further social engineering attacks by user impersonation, blackmail, or coercion. However, generative AI is not used exclusively by bad actors—organizations are increasingly using the same technology to build better cybersecurity defenses.
- **Business Email Compromise (BEC)**— According to the FBI's Internet Crime Complaint Center, BEC is one of the most financially damaging online crimes. It exploits the fact that most businesses rely on email to conduct business. While BEC is not unique to the financial services sector, it continues to be a prevalent means for intercepting payments.
- **Quantum Computing and Cryptographic Risks**— The U.S. government remains concerned with the development and trajectory of quantum information technologies and products that could compromise existing encryption and other cybersecurity controls across critical infrastructure sectors.
- **Ransomware Attacks**— Ransomware is an increasingly serious threat to credit unions. Ransomware attacks continue across all critical infrastructure sectors,

including the financial sector. Ransomware attacks and payments have continued to increase in frequency, scope, and volume and are a lucrative enterprise for cyber criminals. Ransomware as a service is a cybercrime business model in which a ransomware group sells its code or malware to other hackers, who then use it to carry out their own ransomware attacks. CISA's [StopRansomware](#) campaign provides a whole-of-government approach to tackle ransomware more effectively and serves as one central location for ransomware resources and alerts.

- **State-sponsored Cyber Activities** – Over the past year, U.S. government organizations, including CISA, the National Security Agency (NSA), and the FBI continued to produce joint advisories to alert the public that state-sponsored cyber actors' activities against critical infrastructure are a real threat. Along with CISA, the FBI, and the NSA, the NCUA has encouraged credit unions of all sizes to adopt a heightened state of awareness and to proactively hunt threats to defend against this risk. Additionally, the NCUA provided guidance and resources to credit unions to assist in mitigating this threat.
- **Third-party Risk** – Financial institutions, including credit unions, rely on third-party service providers to deliver critical services to their members and back-office operations. The use of third-party service providers may result in inconsistent vendor incident response, supply chain attacks, a lack of credit union visibility into vendor controls and cybersecurity posture.

The speed, quantity, and evolving nature of cybersecurity threats demands constant vigilance from financial services sector entities, agencies, and regulators.

## CONCLUSION

The NCUA is committed to strong cybersecurity resilience within the agency and the credit union system. As the digital landscape continues to evolve, the NCUA will continue adapting its cybersecurity approach to efficiently and effectively address emerging threats and challenges.

## APPENDIX: RESOURCES

### Regulations

Reference
<a href="#">Part 748 – Security Program</a>
<a href="#">Part 749 – Records Preservation Program</a>

### Letters to Credit Unions<sup>8</sup>

Year	Letter	Letters to Credit Unions
2025	25-CU-01	<a href="#">NCUA's 2025 Supervisory Priorities</a>
2025	25-CU-02	<a href="#">Cyber Incident Notification Requirements Update to Letter 23-CU-07</a>
2024	24-CU-02	<a href="#">Board of Director Engagement in Cybersecurity Oversight</a>
2023	23-CU-07	<a href="#">Cyber Incident Notification Requirements</a>

<sup>8</sup> Letters to Credit Unions and other guidance is available on the NCUA website under [Regulation & Supervision](#).