



NCUA
National Credit Union Administration

**OFFICE OF INSPECTOR
GENERAL**

**AUDIT OF THE NCUA'S
CYBER THREAT INFORMATION SHARING**

**Report #OIG-25-07
June 9, 2025**





Pursuant to Pub. L. 117-263 § 5274, non-governmental organizations and business entities identified in this report have the opportunity to submit a written response for the purpose of clarifying or providing additional context to any specific reference. Comments must be submitted to oigmail@ncua.gov within 30 days of the report publication date as reflected on our public website. Any comments will be appended to this report and posted on our public website. We request that submissions be Section 508 compliant and free from any proprietary or otherwise sensitive information. A response that does not satisfy the purpose set forth by the statute will not be attached to the final report.



National Credit Union Administration

Office of Inspector General

SENT BY EMAIL

TO: Distribution List

FROM: Acting Inspector General Marta Erceg

**MARTA
ERCEG**

Digitally signed by
MARTA ERCEG
Date: 2025.06.09
15:13:48 -04'00'

SUBJ: Audit of the NCUA's Cyber Threat Information Sharing

DATE: June 9, 2025

The National Credit Union Administration (NCUA) Office of Inspector General (OIG) conducted this self-initiated audit to assess how effectively the NCUA shared cyber threat information. Our objectives were to determine whether the NCUA: 1) effectively used shared cyber threat information for the supervision of credit unions; and 2) implemented effective processes to share cyber threat information to support credit union and financial system resiliency.

Our audit determined that the NCUA needs to mature its governance processes for cyber threat information sharing to support supervision of credit unions more effectively during a cybersecurity event or incident that may increase risk to the National Credit Union Share Insurance Fund (Share Insurance Fund or SIF) and financial services sector stability. Additionally, the NCUA should improve its ability to acquire, analyze, and use cyber threat information for internal analysis and external response. We made eight recommendations in our report and management agreed to all the recommendations.

We appreciate the cooperation and courtesies NCUA management and staff provided to us during the audit. If you have any questions on the report and its recommendations, please contact me at 703-518-6352.

Distribution:

Chairman Kyle S. Hauptman

Executive Director Larry Fazio

Acting Deputy Executive Director Towanda Brooks

General Counsel Frank Kressman

Chief of Staff Sarah Bang

Office of External Affairs and Communication Director Sierra Robinson

Office of Examination and Insurance Director Kelly Lay

Office of Examination and Insurance Associate Director David Matheu

Office of Continuity and Security Management Director Kelly Gibbs

Attachment



TABLE OF CONTENTS

<u>Section</u>	<u>Page</u>
EXECUTIVE SUMMARY	1
BACKGROUND	2
RESULTS IN DETAIL.....	8
NCUA Should Mature Governance Processes for Cyber Threat Information Sharing	8
NCUA Does Not Effectively Acquire, Analyze, and Use Cyber Threat Information for Supervision.....	12
NCUA Needs Statutory Examination and Oversight Authority Over Third-Party Vendors	15
APPENDICES:	
A. Objective, Scope, and Methodology	17
B. NCUA Management Response	20
C. Acronyms and Abbreviations.....	24



EXECUTIVE SUMMARY

The NCUA OIG conducted this self-initiated audit to assess how effectively the NCUA shared cyber threat information.¹ Our objectives were to determine whether the NCUA: 1) effectively used shared cyber threat information for the supervision of credit unions; and 2) implemented effective processes to share cyber threat information to support credit union and financial system resiliency. The scope of our audit covered cyber threat information sharing from March 1, 2022, through December 31, 2024.

Our audit determined that the NCUA needed to mature its governance processes for cyber threat information sharing to support supervision of credit unions more effectively during a cybersecurity event or incident that may increase risk to the Share Insurance Fund and financial services sector stability. Additionally, NCUA did not effectively acquire, analyze, and use cyber threat information for internal analysis and external response. Finally, NCUA continues to need statutory examination and oversight authority over third-party vendors to be able to effectively assess and monitor third-party cybersecurity exposures.

We are making eight recommendations in our report to address the issues identified.

¹ For the purposes of this audit, the OIG considers cyber threat information to include cyber incidents or other threat information that may address the risk of a potential or immediate systemic impact to the credit union or financial services sector operational resiliency. It is not meant to address individual cyber threat characteristics (such as internet protocol addresses or file names) or information readily available to individual credit unions through public means, unless specifically related to an identified systemic threat.



BACKGROUND

The NCUA is an independent federal agency that insures deposits at federally insured credit unions and charters and regulates federal credit unions. The NCUA protects the safety and soundness of the credit union system by identifying, monitoring, and reducing risks to the SIF, which provides up to \$250,000 of federal share insurance to millions of accounts in all federally insured credit unions. The agency operates a headquarters in Alexandria, Virginia; an Asset Management and Assistance Center in Austin, Texas to liquidate credit unions and recover assets; and three regional offices which carry out the agency's supervision and examination program, along with the Office of National Examinations and Supervision. The NCUA is responsible for the federal regulation and supervision of 4,645 federally insured credit unions with more than \$2.2 trillion in assets across all states and United States territories as of January 2024.²

Cybersecurity threats continue to pose significant risks to the financial services sector and remain one of the NCUA's top supervisory priorities.³ As the credit union system increases its dependency on technology, cybersecurity threats continue to evolve and credit unions of all sizes are potentially vulnerable to cyberattacks. In addition, with the increased reliance on third-party providers, effects could cascade when a cybersecurity incident happens throughout the financial services sector. The interconnected nature of the financial system demonstrates the need for effective and efficient information sharing to build situational awareness and operational resiliency at both the NCUA and credit unions.

The financial services sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions. The NCUA plays a role in maintaining the nation's financial stability and critical infrastructure⁴ resiliency as a member of the Federal Financial Institutions Examination Council (FFIEC) and as a member of the Financial and Banking Information Infrastructure Committee (FBIIC).⁵ In addition, the NCUA Chairman is a voting member of the Financial Stability Oversight Council (FSOC).⁶ As well, the NCUA coordinates with other federal and state regulatory agencies to share threat information and strengthen cybersecurity resiliency.⁷

² 2024 Annual Performance Plan (Jan. 2024).

³ NCUA's 2025 Supervisory Priorities (Jan. 2025).

⁴ Critical infrastructure is defined as the systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters. Exec. Order 13636, Improving Critical Infrastructure Cybersecurity (Feb. 2013).

⁵ The FBIIC serves as the Government Coordinating Council for the Financial Services Sector and provides a forum for financial regulators and the U.S. Department of the Treasury (Treasury) to coordinate critical infrastructure efforts.

⁶ FSOC is an interagency body tasked with identifying and responding to emerging risks and threats to the financial system.

⁷ NCUA's Cybersecurity and Credit Union System Resilience Report (June 2024).



The U.S. Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency (CISA) is the national coordinator for critical infrastructure security and resilience. CISA coordinates with the Sector Risk Management Agencies (SRMAs) to scale coordination across the United States. Treasury is the SRMA for the Financial Services Sector. The requirements and expectations on the protection of critical infrastructure from cybersecurity threats is outlined in and informed by various executive orders, presidential policy directives, rules, plans, and strategies including the following:

- Executive Order 13636, Improving Critical Infrastructure Cybersecurity (2013)
- Presidential Policy Directive-21, Critical Infrastructure Security and Resilience (2013)
- National Infrastructure Protection Plan (NIPP) 2013: Partnering for Critical Infrastructure Security and Resilience (2013)
- Financial Services Sector-Specific Plan 2015 (2015)
- Executive Order 13691, Promoting Private Sector Cybersecurity Information Sharing (2015)
- Critical Infrastructure Threat Information Sharing Framework (2016)
- Cyber Incident Reporting for Critical Infrastructure Act of 2022 (CIRCIA) (2022)
- National Cybersecurity Strategy (2023)
- National Security Memorandum on Critical Infrastructure Security and Resilience (2024)

Overall, these laws, policies, and directives highlight the increased concerns related to cybersecurity threats and the need for communication between and within the public and private sectors to secure critical infrastructure. NIPP 2013 emphasizes the need for critical infrastructure information sharing to gain knowledge of infrastructure risk and interdependencies to build awareness and enable risk-informed decision making while the Financial Services Sector-Specific Plan 2015 identifies information sharing as foundational to achieving sector goals for security and resilience. CIRCIA will require covered entities, such as credit unions, to timely report cyber incidents to CISA when the related rulemaking is finalized and implemented. CISA will share information with incident response stakeholders to strengthen collective defense, improve efforts to identify root causes of incidents, and facilitate federal decision-making and response. Most recently, the National Security Memorandum of Critical Infrastructure Security and Resilience highlighted the essential need for information exchange to enable actions and outcomes that reduce risks.



Cybersecurity Threat Information Sharing Responsibilities

The NCUA receives cyber threat information⁸ from a variety of public and non-public sources. Several NCUA's offices have responsibilities related to evaluating and assessing the sharing of cyber threat information to support supervision purposes including the Office of Examination and Insurance (E&I), the Office of Continuity and Security Management (OCSM), and the Office of the Executive Director (OED).

The Critical Infrastructure Division (CID) within E&I has responsibility for identifying risks arising from threats that may affect the credit union system. CID's responsibilities include cybersecurity and critical infrastructure monitoring, incident reporting, and related interagency work. Additionally, the office develops and provides examiner training for information security examiners. In early 2024, CID proposed, but never finalized, addressing its work into four categories: examination and supervisory strategies; threat intelligence and strategic reporting; education, response, and operational readiness; and partner and engagement.

OCSM has the responsibility to maintain awareness of classified and unclassified intelligence that may affect the NCUA, credit unions, or the financial services sector, and to advise NCUA leadership and offices. OCSM provides threat awareness to credit unions, as appropriate, to support safety and financial soundness. OCSM also provides briefings to NCUA senior staff on relevant intelligence.

Within the OED, the NCUA filled the cybersecurity advisor and coordinator position in 2023 to organize, coordinate, and advise on cybersecurity and critical infrastructure matters across NCUA offices. The cybersecurity advisor and coordinator is responsible for enhancing cyber incident coordination with federal banking agencies, stakeholder outreach and engagement, and supporting cybersecurity information and guidance provided to credit unions and other stakeholders. This position also identifies what is needed to prioritize the safety of the SIF and updates the NCUA Board on cybersecurity threats.

NCUA coordinates with other federal regulatory agencies, including through working groups such as the FFIEC's Cybersecurity Critical Infrastructure Subcommittee (CCIS) and FBIIC, to share cybersecurity threat information. CCIS provides recommendations to the interagency Task Force on Supervision related to cybersecurity, critical infrastructure security, and the resilience of financial institutions and technology service providers. NCUA's coordination with FBIIC includes working with the federal and state financial regulators to address operational and tactical issues related to critical infrastructure matters, including cybersecurity, within the financial services industry. NCUA maintains memorandums of understanding with state supervisory authorities to share information regarding federally insured state-chartered credit

⁸ See footnote #1 for definition of cyber threat information.



unions.

Credit Union Cyber Incident Reporting

NCUA's cyber incident notification requirements for federally insured credit unions were implemented in September of 2023 after the NCUA amended 12 Code of Federal Regulation (CFR) Part 748⁹ to require the notifications. Prior to the amendment, credit unions already were required to notify the appropriate NCUA regional director as soon as possible when the credit union became aware of an incident involving unauthorized access to or use of sensitive member information under 12 CFR Part 748, Appendix B, Section II.A.1b, which the NCUA noted was narrower in scope than the new cybersecurity notification rule. The cyber incident notification rule required federally insured credit unions to notify the NCUA within 72 hours after a credit union reasonably believed that a reportable cyber incident occurred. The rule defined a cyber incident as an occurrence that actually or imminently jeopardizes, without lawful authority, the integrity, confidentiality, or availability of information on an information system or actually or imminently jeopardizes, without lawful authority, an information system. Federally insured credit unions are required to report a cyber incident that leads to one or more of the following:

- A substantial loss of confidentiality, integrity, or availability of a network or member information system that results from the unauthorized access to or exposure of sensitive data, disrupts vital member services, or has a serious impact on the safety and resiliency of operational systems and processes.
- A disruption of business operations, vital member services, or a member information system resulting from a cyberattack or exploitation of vulnerabilities.
- A disruption of business operations or unauthorized access to sensitive data facilitated through, or caused by, a compromise of credit union service organization, cloud service provider, or other third-party data hosting provider or by a supply chain compromise.

Federally insured credit unions may notify the NCUA through a designated phone number, secure email,¹⁰ or, as of January 2025, an online webform.¹¹

The NCUA's National Supervision Policy Manual (NSPM) describes these notification and reporting procedures. E&I's CID is responsible for triaging and tracking reported incidents in the Cyber Incidents Credit Unions Reporting System (CICURS) and is required to request that the region follow up, if warranted. NCUA requests federally insured credit unions to provide as much of the following information as is known at the time of reporting:

⁹ 12 CFR Part 748, Security Program, Suspicious Transactions, Catastrophic Acts, Cyber Incidents, and Bank Secrecy Act Compliance.

¹⁰ Letter to Credit Unions, 23-CU-07, Cyber Incident Notification Requirements (Aug. 2023).

¹¹ Letter to Credit Unions, 25-CU-02, Cyber Incident Notification Requirements Update to Letter 23-CU-07 (Jan. 2025).



- Credit union name and charter number,
- Name, title, and contact information of the individual reporting the incident,
- When the credit union reasonably believed a reportable cyber incident took place, and
- Basic description of the reportable cyber incident, including known impact on functions, potential impact on functions, and whether sensitive information was compromised.

Based on the incident report details provided by the credit union, E&I's CID attempts to identify the following:

- Functional and informational impact,
- Initial access,
- Third-Party determination,
- Service and operational impact,
- Contact information on possible actors responsible,
- Description of exploited vulnerabilities (if applicable), and
- Severity.

E&I's CID provides a monthly report of all cyber incidents to regional offices. Regional Division of Supervision shares the monthly report of cyber incidents to assigned exam staff and specialists and shares a report with all federally insured state credit union cyber incidents with the applicable state supervisory authorities.

(b) (8) Incident

(b) (8) a cloud services provider for credit unions,¹² was hit by a ransomware attack on November 26, 2023. As a result, many credit union customers of **(b) (8)** experienced a service outage. In addition, **(b) (8)**, a critical core processing vendor for credit unions, used **(b) (8)** for its cloud-hosted services. The approximately 60 credit unions affected by the **(b) (8)** outage were small institutions with \$100 million or less in assets. Based on NCUA estimates, approximately \$912 million in aggregate assets and 93,000 members nationwide were at risk by this cyber incident. Upon awareness of the incident and potential magnitude, the NCUA provided updates to Treasury and peer regulators through FBIIC

¹² **(b) (8)** is a subsidiary of **(b) (8)**, which provides disaster recovery and cloud services to the credit union industry.



protocols for a potential sector impact. Additionally, the NCUA informed the Federal Bureau of Investigation and DHS's CISA. The NCUA drafted an after-action report related to this incident.

This incident highlighted several challenges the NCUA faces and areas in need of improvement when supervising credit unions during a cyber incident, such as the need to develop effective communication and response activities, improve information sharing, standardize reporting issues, and manage roles and responsibilities. In addition, the incident demonstrated that the NCUA's lack of third-party vendor authority limited its ability to fully analyze and assess risks posed by vendors and ability to obtain information and fully understand the extent and scope of the attack.

Pre-Victim Notification Event

In July 2024, the NCUA received intelligence indicating a possible threat to credit unions. A pre-victim notification was sent to credit unions in September 2024. The NCUA's actions in response to the potential threat demonstrated the need for policy and process improvement to determine how information is shared with credit unions and external entities, how information is distributed within the agency and thresholds for information sharing, and in NCUA's ability to address potential third-party risks due to the lack of statutory oversight authority.

Third-Party Vendor Reporting

Credit unions are heavily reliant on third-party vendors, who are not subject to the NCUA's oversight authority. However, the cyber incident notification requirements require credit unions to report third-party vendor disruptions or supply chain compromises to the NCUA.

The cyber incident reporting system data demonstrated that approximately 70 percent of the over 1,000 incidents reported between September 1, 2023, and August 31, 2024, were related to third-party vendors. This high number of incidents was tied to 13 specific events, which indicated their wide-spread impact.



RESULTS IN DETAIL

The objectives of our audit were to determine whether the NCUA: 1) effectively used shared cyber threat information for the supervision of credit unions; and 2) implemented effective processes to share cyber threat information to support credit union and financial system resiliency.

Based on our audit work, we determined that the NCUA's processes were not mature enough to demonstrate effective information sharing with credit unions and external partners. The NCUA needs to improve its identification, acquisition, use, and sharing of cyber threat information to inform supervision and strengthen credit union and financial system resiliency. Additionally, the agency did not have sufficient established processes to effectively acquire or utilize cyber threat information within its supervision activities. The NCUA continues to lack oversight authority over third-party vendors, which impacts its ability to effectively monitor and manage vendors' risk exposures.

The detailed results of our audit follow.

NCUA Must Mature Its Governance Processes Around Cyber Threat Information Sharing

We determined the NCUA's governance over cyber threat information sharing needs strengthening. Specifically, we determined that cyber threat information sharing with credit unions was subjective and inconsistent both in methodology and delivery. In addition, the agency did not finalize and implement all 29 recommendations NCUA senior staff and management developed in a draft after-action report related to the (b) (8)

(b) (8) cyber incident. Recommendations included improvements needed in communication protocols, evaluation of current requirements, improved data acquisition and use, new and revised policy and guidance, and updated incident management processes. Finally, we determined cyber threat information sharing roles and responsibilities were not clearly defined in policy, including when action has been delegated to staff or specific management. We believe this weakness in governance may prevent the NCUA from effectively supervising credit unions during a cybersecurity incident, which could result in increased risk to the share insurance fund and financial services sector stability.

Details

Several NCUA offices have cyber threat information sharing responsibilities related to credit union resilience including E&I's CID, OCSM, and OED. We recognize the CID has consistently not been fully staffed and has had numerous management changes, which caused frequent reprioritization of goals and responsibilities. Additionally, CID is accountable to multiple NCUA leadership lines when dealing with critical infrastructure, which has historically made it challenging to prioritize and finalize output and coordinate with peer offices. Although OED hired a cybersecurity advisor and coordinator to support these efforts, continued efforts to mature these coordination processes are still needed.



The NCUA leverages the FBIIC All-Hazards Incident Response Plan's scoring model and severity schema for reporting incidents or threats to Treasury that may significantly affect the financial services sector. The severity and scale of the incident determines the type of reporting expected; however, incident categories are also designed to capture heightened sector or public concern resulting from situations that may not impact financial services or pose a specific threat to the sector at time of activation. The FBIIC protocols, while non-binding, also provide guidance on how the FBIIC can engage other government partners when necessary and appropriate.

When evaluating information to be shared externally to credit unions or to other external stakeholders outside of the established FBIIC protocols for "medium severity" incidents or higher, E&I's CID considers what has been reported within the industry and what has been reported by credit unions to determine alignment. The CID also evaluates if there is a systemic risk and if the incident is controlled or cascading. There is no specific threshold for sharing cyber threat information with credit unions and is primarily based on evaluation in collaboration between leadership within E&I and OED based on experience and professional judgment which may result in inconsistent approaches to cyber threat information sharing. E&I and OED also rely on professional judgment in selecting the method to share information.

Policies and procedures related to the NCUA's response to a cyber incident have not been finalized. The NCUA's NSPM limits the procedures to only address implementation of the cyber incident notification requirements. The NSPM does not provide guidance to E&I on how to fully assess and share analysis of data, as appropriate, but does provide the roles, responsibilities, and requirements of implementing the cyber incident notification requirements.

The NCUA drafted an after-action report on the (b) (8) incident that occurred in November 2023. We determined during our audit this report was never finalized. In that draft report, the NCUA identified numerous breakdowns in cyber threat information sharing that included:

- Inadequate integration between the liquidity playbook and cyber incident playbook, which could delay access to emergency funding,
- Unclear ownership in communication and response activities,
- Difficulties in determining which credit unions were affected due to unreliable information or the inability to obtain information including from regulators with third-party vendor authorities,
- Delayed incident reporting by credit unions,
- Inefficient incident coordination,
- Unclear roles and responsibilities,



- Delayed grant allocation for credit unions,
- Inefficiencies in CICURS, and
- A lack of clear protocols for internal and interagency communication.

Regarding the NCUA's pre-victim notification event, in reviewing the draft lessons learned report, and through discussion with NCUA management, we identified that complications regarding the notification existed due to the following:

- Unclear decision-making authorities regarding how the information should be shared with credit unions,
- Communication protocols with examiners and regulated entities that resulted in credit union concerns,¹³
- A lack of identified threshold and process for information sharing to credit unions and external partners, and
- The inability to address a potential third-party vendor issue due to lack of oversight authority.

As a result, NCUA management has:

- Developed but not finalized policies and procedures related to cyber threat information sharing such as the Cyber Incident Coordination Team Charter, Cyber Incident Instructions, and associated procedures.
- Not clearly established roles and responsibilities, including addressing any necessary delegation of authorities, appropriate communication channels, or single points of failure.
- Not finalized deliverables and action items related to the (b) (8) cyber incident, which has delayed implementation of recommendations addressing identified concerns.
- Not defined the criteria or threshold for information sharing directly with credit unions or external stakeholders. Information was shared inconsistently with credit unions through multiple methods (such as directly through NCUA staff or by an alert) based on staff and management judgment. Information sharing with external stakeholders (including other regulators) was inconsistent in approach and frequency.

¹³ Credit union reaction to the alerts were varied. Many credit unions reached out to the NCUA with concerns that the telephonic alert was a scam or requested additional information. Some credit unions identified the information as not useful while others expressed greater concern and in one case a credit union briefly shut down due to concerns of an imminent threat.



Based on these issues and those identified above, we are making the following three recommendations.

Recommendations

We recommend NCUA management:

1. Develop and finalize policies and procedures that address cyber threat information sharing. These policies and procedures should, at a minimum, include:
 - Formally documenting internal and external sharing practices, clarifying the criteria and threshold to inform individual credit unions or external stakeholders of a cyber threat, and clarifying the method and timing of informing credit unions or external stakeholders.
 - Determining the criteria for internal assessment for escalation and communication of cyber threat information.
2. Formally establish and clarify operational roles and responsibilities across offices for cyber threat information sharing and any delegation of authorities to determine when issues must be escalated. This should, at a minimum, address:
 - Establishing operational responsibilities at all stages of cyber threat-related events, including pre-incident declaration.
 - Clarifying delegation of authorities for efficient and timely decision making and issue escalation.
 - Identifying single point dependencies and addressing appropriate resourcing.
 - Determining appropriate communication and coordination protocols between offices.

Management Response

Management agreed with the recommendations. Management stated that the NCUA will implement a formal policy by September 30, 2026. Management also stated that because other governmental and non-governmental entities are the primary sources of cyber information for credit unions, the policy will reflect that the NCUA will share cyber threat information only when the information is not being provided by another party, may be shared, and is actionable.

OIG Response

We concur with management's planned action.



3. Ensure timely finalization and implementation of recommendations identified in the after-action and lessons learned reports for cyber-related incidents, including the draft (b) (8) after-action report and the draft pre-victim notification lessons learned report.

Management Response

Management agreed with this recommendation. Management stated the NCUA will finalize the reports by March 31, 2026, and implement applicable recommendations within appropriate timeframes.

OIG Response

We concur with management's planned action.

NCUA Does Not Effectively Acquire, Analyze, and Use Cyber Threat Information for Supervision

The NCUA did not effectively acquire, analyze, and use cyber threat information for internal analysis and external response to support credit union supervision. Specifically, we determined the NCUA had incomplete and low-quality data for

credit union reported incidents, underdeveloped data management practices for shared cyber threat information, and had not fully evaluated the usefulness of available resources for cyber threat information such as those available through suspicious activity reports (SARs). The NCUA was unable to determine if its method of sharing cyber threat information within the agency or with credit unions and other external parties was effective or consistent and was unable to determine the quality of the information. Additionally, the NCUA did not effectively use cyber threat information to inform supervision practices and policies. This occurred because NCUA management had not developed a fully formalized, integrated, and established cyber threat information acquisition and analysis program that addressed critical infrastructure concerns for credit union supervision. As a result, NCUA management tasked with organizing, coordinating, and advising on cybersecurity and critical infrastructure matters across all NCUA offices, may not be able to effectively assess and address risks to critical infrastructure and financial services sector stability. Additionally, the NCUA may not be able to effectively collaborate with external partners including Treasury, DHS, and other regulators who have a role in critical infrastructure and financial services sector resilience.

Details

In September 2023, the NCUA began acquiring cyber incident information through voicemails and emails from credit unions in accordance with NCUA's cyber incident notification requirements. Based on this information, CID staff selected the incident description fields from a dropdown menu and input a written description of the incident in CICURS. Through our review of CICURS and interviews with CID staff, we believe staff having to input this information



manually and the lack of clear instructions or procedures for assessing the information in CICURS may cause inconsistencies in system reporting. For example, CID indicated that to prepare the 2024 Annual Cybersecurity and Credit Union Resilience Report, CID reviewed 831 incident reports to validate the initial access field, which revealed data integrity issues related to naming conventions. Additionally, we learned from CID staff that the fields identified for use in initial reporting of incident type were cumbersome because there are 107 different incident types available for staff to select in CICURS. Prior to implementing the cyber incident notification requirements, the NCUA relied upon credit unions to report cyber threat incidents to the regions, which then provided the updates to CID. We determined data from this prior method also did not include complete and consistent data now defined in the cybersecurity incident notification requirements.

The NCUA also acquires information from other stakeholders and external partners. Due to staff changes and underdeveloped data management and retention practices, we were unable to obtain and validate the completeness of cyber threat information shared with the NCUA and therefore could not evaluate whether the NCUA consistently responded timely or effectively to this threat information. Additionally, staff managing Bank Secrecy Act-related priorities did not evaluate SARs for cyber information.¹⁴ Instead, staff indicated that it may be more appropriate for other E&I staff to obtain access and review information if deemed permissible. We confirmed with the NCUA Office of General Counsel that the FinCEN memorandum of understanding with the NCUA would allow authorized E&I staff to review SARs for cyber incidents as part of its appropriate legal authority to supervise and regulate credit unions.

Although we confirmed NCUA offices collaborate in sharing cyber threat information, we also determined the information shared may not always be acted upon. NCUA staff informed us that cyber threat information shared within the agency was not always used and feedback was not consistently provided between offices to determine if the information shared was useful. In addition, we determined that because of the sharing of cyber threat information with credit unions was infrequent and ad hoc, the agency was unable to verify if information shared, including method of sharing and type of information, was helpful to credit unions and therefore may not be an effective deployment of NCUA resources. Finally, NCUA staff and officials informed us there was no formal process to determine how cyber threat information should be used to identify or address any policy gaps or guidance deficiencies within the NCUA's examination and supervision of credit unions.

As previously mentioned, the NCUA's pre-victim notification to credit unions resulted in concerns with how the NCUA shared information with credit unions. Without analysis of appropriate practices for cyber threat information sharing, the NCUA may not be effectively

¹⁴ See Financial Crimes Enforcement Network (FinCEN) Advisory FIN-2016-A005, Advisory to Financial Institutions on Cyber-Events and Cyber-Enabled Crime, which encourages and provides guidance to U.S. financial institutions on SAR reporting of cyber events, and FinCEN Advisory FIN-2021-A004, Advisory on Ransomware and the Use of the Financial System to Facilitate Ransom Payments, which provides additional filing instructions related to cyber events.



acquiring, sharing, and using information needed by internal and external stakeholders to assess the risk of cyber threats.

Based on the issues identified above, we are making the following five recommendations.

Recommendations

We recommend NCUA management:

4. Update and document incident reporting triage protocols to provide consistent and useable data in the Cyber Incidents for Credit Unions Reporting System.

Management Response

Management agreed with the recommendation. Management stated that the NCUA updated the categorization framework and will incorporate enhanced quality assurance into protocols by March 31, 2026.

OIG Response

We concur with management's planned action.

5. Document and implement internal data management protocols that ensure the appropriate sharing, assessment, and response of available cyber threat information.

Management Response

Management agreed with the recommendation. Management will update protocols by March 31, 2026, to include maintaining a log to record the dissemination of information and sharing of cyber threat information to applicable staff within the agency. Additionally, management described how NCUA collects and uses cyber threat information and listed data management and information sharing protocols it had instituted.

OIG Response

We concur with management's planned action.

6. Evaluate and determine if cyber threat information in suspicious activity reports should be used in NCUA's general examination and supervision of credit unions.

Management Response

Management agreed with the recommendation. Management indicated that the NCUA evaluated suspicious activity reports filed in 2024 and determined that only .31 percent of reports involved a cyber event against a credit union. Thus, management determined that conducting analysis



would provide no measurable benefit and considers this recommendation complete.

OIG Response

We concur with management's completed action. We will review evidence of the completed action to determine closure of this recommendation.

7. Develop a process to assess credit unions' and other stakeholders' feedback on NCUA's cyber threat information sharing and update information sharing processes to reflect any necessary changes.

Management Response

Management agreed with the recommendation. Management will document procedures for sending feedback to the applicable office in its policy by September 30, 2026.

OIG Response

We concur with management's planned action.

8. Ensure the Office of Examination and Insurance provides timely updates to examination and supervisory guidance to address cyber risks.

Management Response

Management agreed with the recommendation. Management indicated that the Office of Examination and Insurance will ensure responsible subject matter staff are fully informed of and operate consistent with the expectations for updating examination and supervisory guidance to address cyber risks.

OIG Response

We concur with management's planned action. We will close the recommendation when we confirm the action has been adequately implemented.

NCUA Must Continue to Pursue Statutory Third-Party Vendor Authority

The NCUA continues to not have oversight authority over third-party vendors of credit unions, unlike bank regulators for bank vendors, and is therefore unable to directly obtain timely and reliable information from third-party vendors. The inability to directly obtain information affects NCUA's ability to effectively supervise, communicate, and enforce corrective action when an incident occurs. As credit unions are part of the financial services sector, risks posed by a significant incident at a third-party vendor of credit unions could impact the nation's critical economic infrastructure and national security.



Details

As previously mentioned, credit union vendor (b) (8) suffered a ransomware attack on November 26, 2023. (b) (8) provides disaster recovery and cloud services to the credit union industry. (b) (8), a critical core processing vendor for credit unions, used (b) (8) for its cloud-hosting services. The ransomware attack caused a service outage that impacted 60 credit unions, causing a prolonged outage of their data processing systems. The NCUA estimated that approximately \$912 million in aggregate assets and 93,000 members nationwide were operationally impacted by the cyber incident.

As noted in our 2020 Audit of NCUA's Examination and Oversight Authority over Credit Union Service Organizations and Vendors (OIG-20-07), the NCUA does not have oversight authority over credit union vendors. This lack of authority limited the agency's ability to initially acquire data and understand the magnitude and scope of impact of the ransomware attack. Vendors are not required to provide information to the NCUA and the NCUA was unable to effectively leverage authorities of bank regulators to obtain information about the attack because (b) (8) (b) (8) primarily services the credit union industry. As a result, bank regulators did not have oversight of the ransomware attack. Additionally, we learned other agencies and state supervisors with vendor oversight authorities were not positioned to gather sufficient information about the attack to provide to the NCUA.

Similarly, regarding the pre-victim notification event, a lack of vendor authority limited the NCUA's response to this potential threat because it was unable to obtain information from a credit union service organization that may have been compromised.

The NCUA continues to need statutory examination and oversight authority over third-party vendors to be able to effectively assess and monitor third-party cybersecurity exposures. The NCUA should continue its efforts to obtain third-party vendor authority as recommended in *OIG Report* *OIG-20-07*.¹⁵ As such, we are not making any new recommendations on this issue.

¹⁵ This deficiency has also been identified by Government Accountability Office, FSOC, and by the NCUA.



Appendix A

OBJECTIVE, SCOPE, AND METHODOLOGY

We developed our objectives for this engagement based on OIG's 2024 Annual Work Plan. Specifically, our objectives were to determine whether the NCUA: 1) effectively used shared cyber threat information for the supervision of credit unions; and 2) implemented effective processes to share cyber threat information to support credit union and financial system resiliency.

To accomplish our audit, we performed fieldwork between April 2024 through April 2025 with information related to the NCUA's cyber threat information sharing.

The scope covered cyber threat information sharing activities from March 1, 2022, through December 31, 2024,¹⁶ and all applicable procedures, documentation, and controls. For the purposes of this audit, the OIG considers cyber threat information to include cyber incidents or other threat information that may address the risk of a potential or immediate systemic impact to the credit union or financial services sector operational resiliency. It is not meant to address individual cyber threat characteristics (such as internet protocol addresses or file names) or information readily available to individual credit unions through public means, unless specifically related to an identified systemic threat.

To achieve our objectives, we performed the following:

- Identified and reviewed federal guidance and requirement for cyber threat information sharing as it related to supervision, credit unions, and financial system resiliency.
- Conducted interviews with NCUA staff and management with cyber threat information sharing responsibilities related to supervision, credit unions, and financial system resiliency.
- Identified sources of cyber threat information sharing related to supervision, credit unions, and financial system resiliency.
- Evaluated NCUA policies and procedures for cyber threat information sharing related to supervision, credit unions, and financial system resiliency.
- Reviewed documentation related to cyber threat information shared internally and externally related to supervision, credit unions, and financial system resiliency.
- Identified third-party exposure considerations.

¹⁶ The scope period was extended from March 1, 2024, to December 31, 2024, to include evaluation of the pre-victim notification event.



- Evaluated internal controls.

Due to agency staffing issues and underdeveloped data management practices, which resulted in a lack of completeness and availability of cyber threat information obtained and shared, we were unable to obtain sufficient data to complete testing. As a result, we identified numerous control deficiencies. In addition, management was unable to assert completeness of information shared by Treasury with the NCUA, or the completeness and accuracy of cyber incidents reported by the credit unions during the scope period. We did not otherwise significantly rely on computer-processed data to answer the audit objectives. Although we obtained data generated from NCUA systems, such as a listing of incidents in CICURS, we relied on our analysis of information from interviews, policies, and procedures to evaluate the data and support our conclusions.

We conducted this audit from April 2024 through April 2025 in accordance with generally accepted government auditing standards and included such tests of internal controls as we considered necessary under the circumstances. Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives. We assessed the effectiveness of the internal controls and determined they were significant to the audit objectives. Specifically, we assessed 5 of the 5 internal control Components and 13 of the 17 associated underlying principles defined in the Government Accountability Office's Standards for Internal Control in the Federal Government.¹⁷

We summarize in Table 1 below the components and principles we assessed.

Table 1: Internal Control Components and Underlying Principles Assessed

Component #1: Control Environment
Principle #3 – Establish Structure, Responsibility, and Authority
Principle #4 – Demonstrate Commitment to Competence
Component #2: Risk Assessment
Principle #6 – Define Objectives and Risk Tolerances
Principle #7 – Identify, Analyze, and Respond to Risk
Principle #9 – Identify, Analyze, and Respond to Change
Component #3: Control Activities
Principle #10 – Design Control Activities
Principle #11 – Design Activities for the Information System
Principle #12 – Implement Control Activities
Component #4: Information and Communication

¹⁷ The Standards for Internal Control in the Federal Government organizes internal control through a hierarchical structure of 5 components and 17 principles. The five components, which represent the highest level of the hierarchy, consist of the Control Environment, Risk Assessment, Control Activities, Information and Communication, and Monitoring. The 17 principles support the effective design, implementation, and operation of the components, and represent the requirements for establishing an effective internal control system.



Principle #13 – Use Quality Information
Principle #14 – Communicate Internally
Principle #15 – Communicate Externally
Component #5: Monitoring
Principle #16 – Perform Monitoring Activities
Principle #17 – Evaluate Issues and Remediate Deficiencies

The report presents within the findings the internal control deficiency we identified. However, because our audit was focused on these significant internal controls, components, and underlying principles, it may not have disclosed all internal control deficiencies that may have existed at the time of this audit.



Appendix B


NCUA MANAGEMENT RESPONSE



National Credit Union Administration
Office of Executive Director

OEI/MJT:mjt
SSIC 1920

SENT BY EMAIL

TO: Acting Inspector General Marta Erceg
FROM: Executive Director Larry Fazio  LARRY FAZIO
SUBJ: Management Response – Cyber Threat Information Sharing Audit
DATE: June 6, 2025

Thank you for the opportunity to review the Office of Inspector General's draft report *Audit of the NCUA's Cyber Threat Information Sharing*. The report includes eight recommendations.

Recommendation 1: Develop and finalize policies and procedures that address cyber threat information sharing. These policies and procedures should, at a minimum, include:

- Formally documenting internal and external sharing practices, clarifying the criteria and threshold to inform individual credit unions or external stakeholders of a cyber threat, and clarifying the method and timing of informing credit unions or external stakeholders, and
- Determining the criteria for internal assessment for escalation and communication of cyber threat information.

Recommendation 2: Formally establish and clarify operational roles and responsibilities across offices for cyber threat information sharing and any delegation of authorities to determine when issues must be escalated. This should, at a minimum, address:

- Establishing operational responsibilities at all stages of cyber threat-related events, including pre-incident declaration.
- Clarifying delegation of authorities for efficient and timely decision making and issue escalation.
- Identifying single point dependencies and addressing appropriate resourcing, and
- Determining appropriate communication and coordination protocols between offices.

Management Response to Recommendations 1 and 2: Management concurs. The NCUA will implement a formal policy by September 30, 2026. The Instruction will provide overall guidance, include roles and responsibilities, and incorporate the existing process to evaluate and prioritize potential risks or incidents by categorizing them based on their severity and impact once a credit union cyber incident is reported. The assessment determines how the agency responds and communicates internally and externally.

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320



Page 2

Please note that several governmental and non-governmental entities are the primary sources of cyber threat information for credit unions. For example, the Department of the Treasury, the Federal Bureau of Investigation (FBI), and the Cybersecurity and Infrastructure Security Agency (CISA) are the authorities over sector-wide communications and response. In addition to these government agencies, there are at least two non-governmental organizations that credit unions can engage to receive information about cyber threats.

As such, the NCUA's role in sharing cyber threat information is generally limited to the infrequent instances when the NCUA has information that can be shared, is actionable, and is not being provided by another party. The NCUA's policy will reflect this.

Recommendation 3: Ensure timely finalization and implementation of recommendations identified in the after-action and lessons learned reports for cyber-related incidents, including the draft Ongoing Operations after-action report and the draft pre-victim notification lessons learned report.

Management Response to Recommendation 3: Management concurs. The NCUA will finalize the reports by March 31, 2026, and implement any recommendations determined to be warranted based on sensible timetables for each recommendation.

Recommendation 4: Update and document incident reporting triage protocols to provide consistent and useable data in the Cyber Incidents for Credit Unions Reporting System.

Management Response to Recommendation 4: Management concurs and will complete this by March 31, 2026. The NCUA has updated the categorization framework for the incident reporting after the audit began and will incorporate enhanced quality assurance into the protocols. As noted in the preamble to the cyber incident reporting final rule, credit unions are not required to include a lengthy assessment of the incident or structured data. Requiring only high-level information through various delivery channels, including email and voice message, reduces the burden and facilitates reporting during a period where credit union management is focused on incident remediation. In January 2025 the NCUA included a web-based form as a convenient and secure method for credit unions to report cyber incidents. The system enhancements provided improved data quality and incident categorization.

Recommendation 5: Document and implement internal data management protocols that ensure the appropriate sharing, assessment, and response of available cyber threat information.

Management Response to Recommendation 5: Management concurs. The protocols will be updated accordingly by March 31, 2026. This will include maintaining a log to record the dissemination and sharing of cyber threat information to applicable staff within the agency.



Page 3

As specified in the rule, cyber threat information is only used to address the risk of a potential or immediate systemic impact to credit unions or the financial services sector. Therefore, cyber threat information is not collected for the intended purpose of sharing with credit unions or even broadly within the NCUA, and only with other government agencies when warranted. The protocols will reflect this.

Please note, since the rule was implemented, the NCUA instituted the following data management and information sharing protocols:

- Cyber incident report data has a records retention schedule;
- The National Supervision Policy Manual (v20.1 and later) includes information on the Cyber Incident Notification Requirements rule roles and responsibilities;
- Monthly reports are disseminated in accordance with the National Supervision Policy Manual;
- Cyber incident report processing uses standardized templates; and
- The Office of Examination and Insurance, Office of Continuity and Security Management, and the Office of the Executive Director actively share and collaborate through a secure portal.

Recommendation 6: Evaluate and determine if cyber threat information in suspicious activity reports (SARs) should be used in NCUA's general examination and supervision of credit unions.

Management Response to Recommendation 6: Management concurs and has completed this evaluation. Since the audit began, the NCUA evaluated the nearly 300,000 suspicious activity reports (SARs) filed in 2024. Only 0.31 percent of SARs indicated some type of cyber event against a credit union. As mining this information is a very resource intensive process that yields limited useful information, management has determined not to use it for this purpose.

Recommendation 7: Develop a process to assess credit unions' and other stakeholders' feedback on NCUA's cyber threat information sharing and update information sharing processes to reflect any necessary changes.

Management Response to Recommendation 7: Management concurs and will document current procedures for sending any such feedback received to the applicable office for consideration in the forthcoming instruction by September 30, 2026.

Recommendation 8: Ensure the Office of Examination and Insurance provides timely updates to examination and supervisory guidance to address cyber risks.



Page 4

Management Response to Recommendation 8: Management concurs. The Office of Examination and Insurance's leadership will ensure its responsible subject matter staff are fully informed of and operate consistent with the expectations for updating examination and supervisory guidance to address cyber risks. This includes continuing the following efforts:

- annual updates to the NCUA's examination scope and supervisory priorities.
- periodic updates to the *Examiner's Guide* and the *National Supervision and Policy Manual*.
- communications with credit unions as warranted, such as cybersecurity alerts, webinars, and updates to the cybersecurity page on NCUA.gov.

Thank you for the opportunity to comment. If you have any questions regarding this response, please contact Shameka Sutton at (703) 548-2485 or ssutton@ncua.gov.



Appendix C

ACRONYMS AND ABBREVIATIONS

Acronym	Term
CCIS	Cybersecurity and Critical Infrastructure Subcommittee
CFR	Code of Federal Regulation
CICURS	Cyber Incidents for Credit Unions Reporting System
CID	Critical Infrastructure Division
CIRCA	Cyber Incident Report for Critical Infrastructure Act
CISA	Cybersecurity and Infrastructure Security Agency
CU	Credit Union
DHS	Department of Homeland Security
E&I	Office of Examination and Insurance
FBIIC	Financial and Banking Information Infrastructure Committee
FFIEC	Federal Financial Institutions Examination Council
FinCEN	Financial Crimes Enforcement Network
FSOC	Financial Stability Oversight Council
NCUA	National Credit Union Administration
NIPP	National Infrastructure Protection Plan
NSPM	National Supervision Policy Manual
OCSM	Office of Continuity and Security Management
OED	Office of the Executive Director
OIG	Office of Inspector General
SARs	Suspicious Activity Reports
Share Insurance Fund	National Credit Union Share Insurance Fund
SIF	National Credit Union Share Insurance Fund



Acronym	Term
SRMA	Sector Risk Management Agency
Treasury	U.S. Department of the Treasury