



NCUA
National Credit Union Administration

OFFICE OF INSPECTOR
GENERAL



Semiannual Report to Congress

April 1, 2025 – September 30, 2025

[This page intentionally left blank]



April 1, 2025 - September 30, 2025

Table of Contents

A Message from the Inspector General.....	1
The National Credit Union Administration Mission.....	2
Introduction.....	3
Federally Insured Credit Union Highlights.....	5
Legislative Highlights.....	7
Office of Inspector General.....	8
Audit Activity.....	9
Peer Reviews.....	22
Investigative Activity	23
Reviews of Legislation, Regulations, and Policies.....	26
Table I : Issued Reports With Questioned Costs.....	27
Table II: Issued Reports with Recommendations that Funds Be Put To Better Use.....	28
Table III: Summary Of OIG Audit Activity during the Reporting Period	28
Table IV: Summary Of OIG Audits In Progress	28
Index of Reporting Requirements.....	29
APPENDICES:	
A. System Review Report (Peer Review of NCUA OIG)	31

[This page intentionally left blank]



April 1, 2025 - September 30, 2025

A Message from the Inspector General

On behalf of the Office of Inspector General (OIG) of the National Credit Union Administration (NCUA), I am pleased to present our Semiannual Report to Congress highlighting our accomplishments and ongoing work for the 6-month period ending September 30, 2025. Our work reflects the legislative mandate of the Inspector General Act to promote the economy, efficiency, and effectiveness of NCUA programs and operations, and protect against fraud, waste, and abuse. The audits and investigations highlighted in this report demonstrate our commitment to that mandate. We issued an audit report on the NCUA's Cyber Threat Information Sharing, which is described later in this report. We continued to work on five investigations opened in prior periods with three different U.S. Attorney's Offices.

The NCUA Board and management were responsive to all OIG recommendations and identified actions to timely implement them. I greatly appreciate the support for our office by the Board and management, including since I became Acting Inspector General in May. I hope that the OIG's audits, investigations, and other work may assist the Board and management in their efforts to streamline the agency while ensuring its continued effectiveness in carrying out its mission and operations.

MARTA
ERCEG

Digitally signed by
MARTA ERCEG
Date: 2025.10.22
12:36:37 -04'00'

Marta Erceg
Acting Inspector General

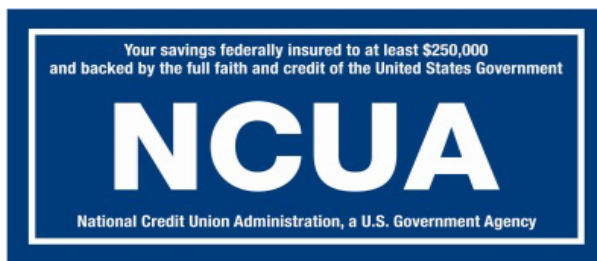


April 1, 2025 - September 30, 2025

The National Credit Union Administration Mission

The National Credit Union Administration's (NCUA) mission is to protect the system of cooperative credit and its member-owners through effective chartering, supervision, regulation, and insurance.

The NCUA protects the safety and soundness of the credit union system by identifying, monitoring, and reducing risks to the National Credit Union Share Insurance Fund. Backed by the full faith and credit of the United States, the Share Insurance Fund provides up to \$250,000 of federal share insurance to millions of account holders in all federal credit unions and the overwhelming majority of state-chartered credit unions.



The Office of Inspector General Mission

The Office of Inspector General (OIG) promotes the economy, efficiency, and effectiveness of NCUA programs and operations, and detects and deters fraud, waste, and abuse, thereby supporting the NCUA's mission of monitoring and promoting safe and sound federally insured credit unions.

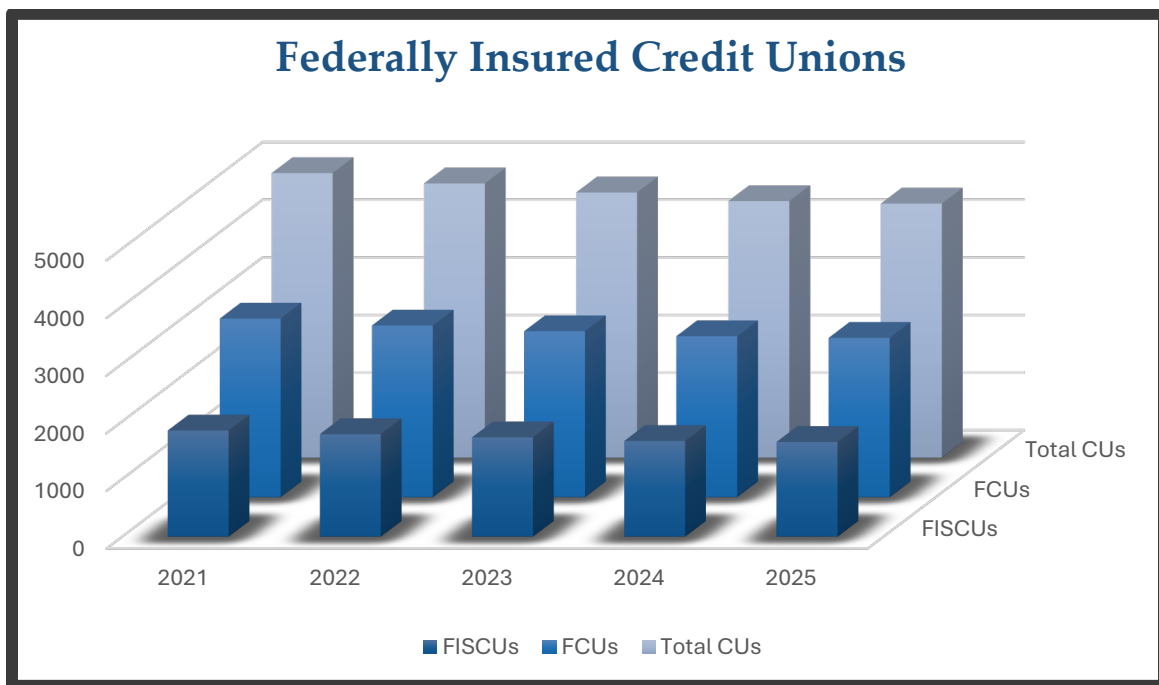
We accomplish our mission by conducting independent audits, investigations, and other activities, and by keeping the NCUA Board and the Congress fully and currently informed of our work.



April 1, 2025 - September 30, 2025

Introduction

The NCUA was established as an independent federal regulatory agency on March 10, 1970. The agency is responsible for chartering, examining, supervising, and insuring federal credit unions. It also insures state-chartered credit unions that have applied for insurance and have met National Credit Union Share Insurance requirements. The NCUA is funded by the credit unions it supervises and insures. As of June 30, 2025, the NCUA supervised and insured 2,740 federal credit unions and insured 1,630 state-chartered credit unions, a total of 4,370 credit unions. This represents a decline of 94 federal and 69 state-chartered credit unions since June 30, 2025, for a total decrease of 163 credit unions nationwide. The year-over-year decline is consistent with long-running industry consolidation trends.

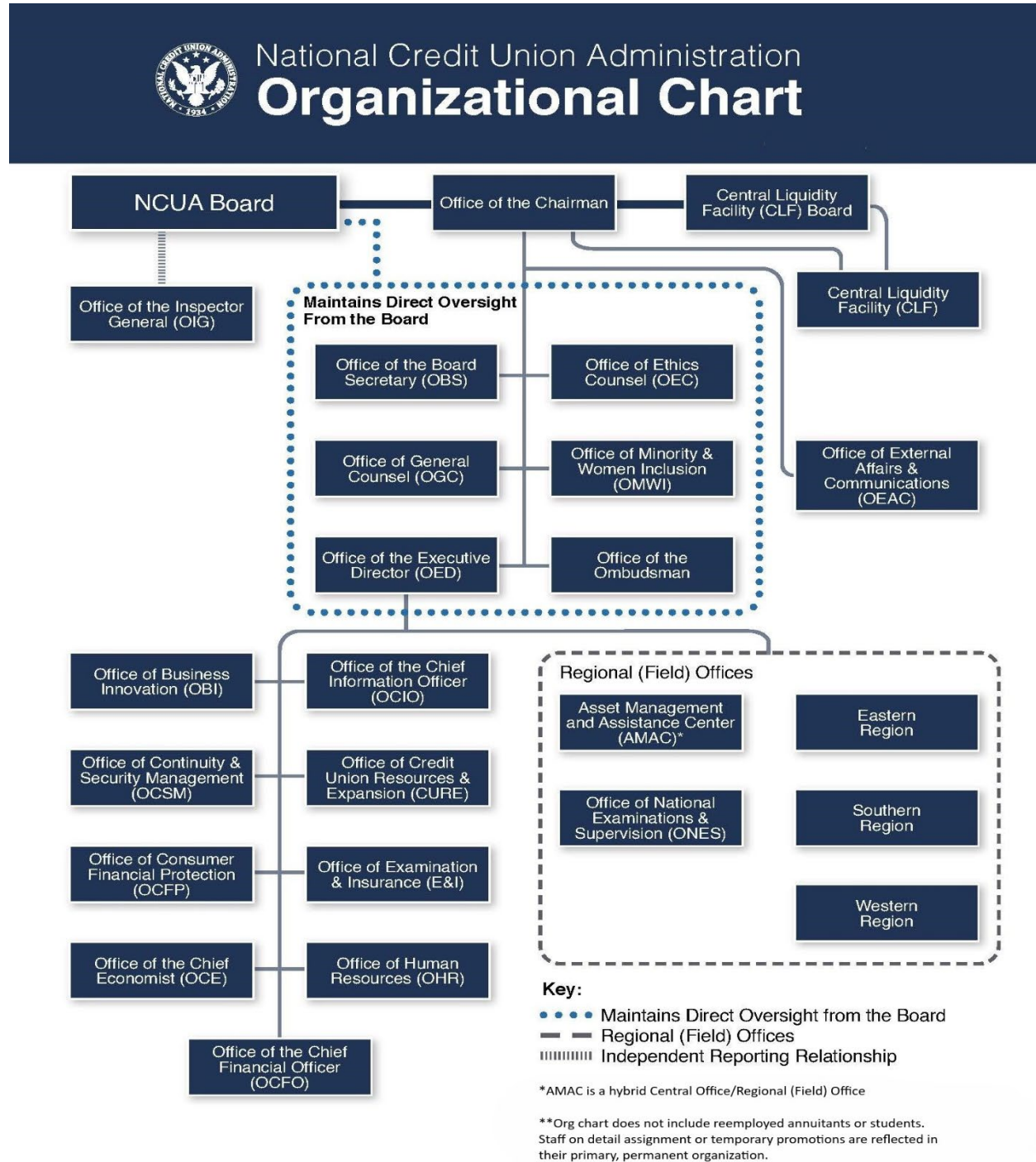


The Federal Credit Union Act provides that the management of the NCUA is vested in a Board consisting of three members appointed by the President and confirmed by the Senate. The Board currently has one member, Chairman Kyle S. Hauptman. The Federal Credit Union Act provides that the Board Chairman shall be the spokesperson for the Board, shall represent the Board and the NCUA in its official relations with other branches of the Government, and shall direct the implementation of the adopted policies and regulations of the Board.



April 1, 2025 - September 30, 2025

The NCUA executes its program through its Alexandria, Virginia central office and regional offices in Alexandria, Virginia (Eastern); Austin, Texas (Southern); and Tempe, Arizona (Western). The NCUA also operates the Asset Management and Assistance Center (AMAC) in Austin, Texas. Please refer to the NCUA's organizational chart below.





April 1, 2025 - September 30, 2025

Federally Insured Credit Union Highlights

Credit unions complete and submit quarterly call reports that contain financial and statistical data to the NCUA. Based on data compiled from these call reports, the NCUA produces a quarterly credit union data summary report¹ and a quarterly financial trend report.² The quarterly data summary report provides an overview of credit union financial performance and includes listings of summarized accounts, selected performance indicators, performance by asset category, as well as balance sheet and income statement details. The financial trends report presents year-to-date financial trends in various chart formats. Following is our summary of the June 30, 2025, quarterly data summary and financial trends reports.

Key Financial Indicators

The June 30, 2025, quarterly data summary report provided a comparison of the second quarter 2025 data to the same quarter in the previous year. For major balance sheet items and key ratios, the report presented the following percentage changes over four quarters (June 2024 to June 2025) for the nation's 4,370 federally insured credit unions: total assets increased by 3.6 percent, net worth ratio increased from 10.84 percent to 11.11 percent, and the loan-to-share ratio decreased from 84 percent to 83.1 percent. The delinquency rate increased from .84 percent to .91 percent. Credit union return on average assets increased from .69 percent to .76 percent.

Share Trends and Distribution

Total shares and deposits increased 5 percent, \$95.45 billion, bringing the balance to \$2.02 trillion. Regular shares accounted for 28.3 percent of total shares and deposits, \$572.98 billion. Money market shares comprised 17.5 percent, \$354.5 billion. Share drafts accounted for 19.3 percent, \$390.81 billion. Share certificates represented 28.5 percent, \$577.22 billion. IRA/Keogh accounts comprised 4.4 percent, \$87.99 billion; non-member deposits comprised 1.2 percent, \$24.73 billion; and all other shares comprised .7 percent, \$13.82 billion of total shares and deposits.

¹ <https://www.ncua.gov/analysis/credit-union-corporate-call-report-data/quarterly-data-summary-reports>

² <https://www.ncua.gov/analysis/credit-union-corporate-call-report-data/financial-trends-federally-insured-credit-unions>



April 1, 2025 - September 30, 2025

Loan Trends and Distribution

Total loans increased 3.9 percent, \$63.58 billion, bringing the balance to \$1.68 trillion. First mortgage real estate loans accounted for the largest single asset category of outstanding loans with \$607.78 billion, 36.1 percent of total loans. Used vehicle loans of \$320.98 billion represented 19.1 percent, while new vehicle loans amounted to \$162.51 billion, 9.7 percent. Other real estate loans of \$167.7 billion accounted for 10 percent. Unsecured credit cards totaled \$85.067 billion, 5.1 percent, while all other unsecured loans totaled \$70.7 billion, 4.2 percent. Leases receivable and all other non-commercial loans represented \$83.33 billion, 5.0 percent. Commercial real estate secured loans totaled \$170.02 billion, 10.1 percent, and commercial non real estate secured loans totaled \$13.2 billion, .8 percent, of total loans.



April 1, 2025 - September 30, 2025

Legislative Highlights

One Big Beautiful Bill Extends Pandemic Response Accountability Committee

On July 4, 2025, the President signed H.R. 1, One Big Beautiful Bill Act, into law as Public Law 119-21. Among many other provisions of the Act, it extends the Pandemic Response Accountability Committee (PRAC) until 2034 and authorizes \$88 million “out of any money in the Treasury not otherwise appropriated” to be used by the PRAC “until expended.” The language also expands the PRAC’s jurisdiction by amending the CARES Act (Pub. L. 116–136), which currently states the PRAC has jurisdiction to “conduct and support oversight of covered funds,” to include any funds made available under Public Law 119-21. However, as of September 30, 2025, the Office of Management and Budget (OMB) had not apportioned these funds to the PRAC for its FY 2026 operations. The PRAC is a committee of the Council of the Inspectors General on Integrity and Efficiency (CIGIE). OMB also withheld the apportionment of appropriated funds for CIGIE’s FY 2026 operations.

GENIUS Act Creates Regulatory Framework for Payment Stablecoins

On July 18, 2024, the President signed S. 1582, Guiding and Establishing National Innovation for U.S. Stablecoins Act (GENIUS Act), into law as Public Law 119-27. This bill establishes a regulatory framework for payment stablecoins (digital assets that an issuer must redeem for a fixed value). Permitted issuers must be a subsidiary of an insured depository institution, a federal-qualified nonbank payment stablecoin issuer, or a state-qualified payment stablecoin issuer. Only permitted issuers may issue a payment stablecoin for use by U.S. persons, subject to certain exceptions and safe harbors. Permitted issuers must be regulated by the appropriate federal or state regulator, such as the NCUA for subsidiaries of credit unions.



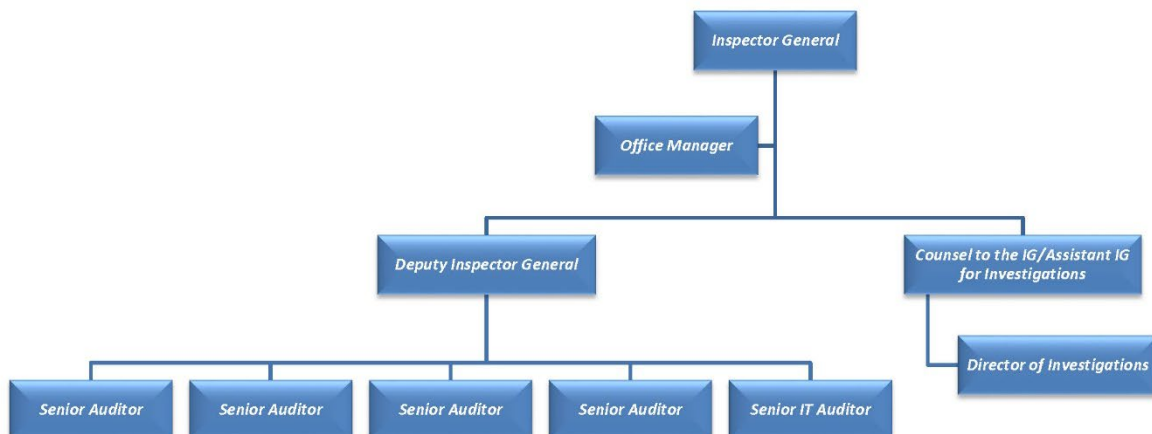
April 1, 2025 - September 30, 2025

Office of Inspector General

The Office of Inspector General (OIG) was established at the NCUA in 1989 pursuant to an amendment of the Inspector General Act of 1978. The Inspector General reports to and is under the general supervision of the NCUA Board. The OIG is responsible for conducting, supervising, and coordinating audits and investigations relating to NCUA programs and operations; recommending policies for and conducting other activities for the purpose of promoting economy and efficiency in the administration of, or preventing fraud and abuse in, NCUA programs and operations; reviewing existing and proposed legislation and regulations to evaluate their impact on the economic and efficient administration of, or the prevention and detection of fraud and abuse in, NCUA programs and operations; and keeping the NCUA Board and the Congress informed of fraud and other serious problems, abuses, and deficiencies, and recommending corrective actions and the NCUA's progress in implementing the corrective actions.

During most of this reporting period, the OIG had seven employees: Counsel to the Inspector General/Assistant Inspector General for Investigations (acting as Inspector General), Senior Information Technology Auditor (acting as Deputy Inspector General), Director of Investigations, three Senior Auditors, and an Office Manager. The chart below represents the OIG's authorized positions, three of which are vacant (Inspector General, Deputy Inspector General, and Senior Auditor) due to departures under the deferred resignation program and the government hiring freeze.

NCUA OIG ORGANIZATIONAL CHART





April 1, 2025 - September 30, 2025

Audit Activity

Audit Reports Issued

OIG-25-07 Audit of the NCUA's Cyber Threat Information Sharing

We conducted this self-initiated audit to determine whether the NCUA effectively used shared cyber threat information for the supervision of credit unions and implemented effective processes to share cyber threat information to support credit union and financial system resiliency. 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. We also determined that the NCUA did not effectively acquire, analyze, and use cyber threat information for internal analysis and external response. We made eight recommendations, including that management develop and finalize policies and procedures that address cyber threat information sharing. Management agreed with all eight recommendations.

OIG-25-08 FY 2025 Independent Audit of the NCUA's Compliance with the Federal Information Security Modernization Act (FISMA) of 2014

We contracted with and supervised the independent public accounting firm Sikich LLC to independently evaluate the NCUA's information security program for compliance with FISMA. For this year's review, OMB required evaluation of 20 core and 5 supplemental reporting metrics in the following 6 security function areas and related domains to assess the maturity level and the effectiveness of agency information security programs: Govern, Identify, Protect, Detect, Respond, and Recover. The maturity levels from lowest to highest were: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. Managed and Measurable and Optimized are considered effective maturity levels.

Sikich concluded that the NCUA implemented an effective information security program by achieving an overall Managed and Measurable maturity level, complied with FISMA, and substantially complied with agency information security and privacy policies and procedures. Although Sikich concluded that the information security program was effective overall, it found that the NCUA's implementation of a subset of selected controls was not fully effective based on its identifying five new weaknesses related to the Govern Function—Cybersecurity Governance Domain; Identify Function—Risk and Asset Management Domain; Protect Function—Configuration Management Domain; and Protect Function—Identity and Access Management Domain. As a result, Sikich made 10 new recommendations to assist the NCUA in strengthening



April 1, 2025 - September 30, 2025

its information security program and practices. In addition, three FISMA recommendations from prior years remain open.

Audits in Progress

Audit of the NCUA's Information Technology Asset Sanitization Process

The NCUA has access to sensitive information that may include information about a person or organization that is not public information, including nonpublic personally identifiable information. Improper disclosure of this information could result in harm to an NCUA employee, credit union, consumer, or other parties external to the NCUA. The NCUA must ensure this information is properly secured to prevent disclosure to unauthorized parties.

NCUA's information security practice includes agency-wide and program-specific policies and procedures for collecting, securing (data is encrypted in transit and at rest), retaining, and destroying data. The NCUA has designated the Senior Agency Information Security/Risk Officer and the Senior Agency Official for Privacy to manage the development, documentation, and dissemination of the media protection policy and procedures. According to its media protection policy, the NCUA must sanitize all digital and non-digital system media using approved equipment, techniques, and procedures prior to disposal, release out of organizational control, or release for reuse in accordance with applicable federal and organizational standards and policies.

We are conducting this self-initiated audit to determine whether the NCUA adequately managed and sanitized its IT assets before disposal or reuse.

Audit of the NCUA's Travel Card Program

The Travel and Transportation Reform Act of 1998 (Public Law 105-264) mandates that federal employees use the government travel charge card for all payments of expenses related to official government travel, unless exempted by the employing agency or the General Services Administration (GSA). The GSA provides charge card services to the entire federal government under a contract, currently the SmartPay 3 contract.

The Government Charge Card Abuse Prevention Act of 2012 requires agency officials to establish and maintain internal controls to ensure the proper use of travel charge cards. In addition, the Act requires that the agency's OIG perform periodic analyses or audits, as necessary, of travel card transactions designed to identify potentially illegal, improper, or erroneous uses of travel cards, and any patterns of such uses. OMB Circular A-123, Appendix B establishes standard minimum requirements and best practices for government charge card



April 1, 2025 - September 30, 2025

programs that may be supplemented by individual agency policies and procedures. The NCUA requires employees' use of travel cards to comply with its travel program policies, the Travel Card Manual, and Public Law 105-264.

We are conducting this self-initiated audit to determine whether the NCUA's travel card policies and procedures are effective in preventing and detecting illegal, improper, or erroneous purchases and payments.

Audit of the NCUA's Field Employees' Duty Station and Work Activities

NCUA employees work in the NCUA's Headquarters or in at various locations in its Regions. An employee's official duty station and associated locality pay are listed on their SF-50. For field employees, the official duty station is the geographic limits of the official duty station designated on the SF-50. Field employees are considered mobile workers whose work is characterized by routine and regular travel to conduct work as opposed to a single authorized worksite. In addition to affecting locality pay, a field employee's official duty station affects travel reimbursement.

On August 9, 2023, NCUA management issued a memorandum and job aid titled "Field Staff Travel Time and Reimbursement Related to the Assigned Official Duty Station" to provide additional clarification regarding the NCUA's travel and commuting policies for field employees, including that field employees are generally expected to live in their official duty station or within reasonable proximity to the official duty station. Management issued this memorandum and job aid because a field employee's residence affects travel reimbursement if they live more than 40 miles from their official duty station and to make clear that an employee's residence is where they live and receive mail daily, and that vacation homes, other family residences, and post office boxes not associated with a physical address were not acceptable alternatives.

We are conducting this self-initiated audit to determine whether the NCUA consistently followed laws, regulations, policies, and procedures in the assignment of a field employees' official duty station, locality pay, and reimbursement for travel.

Audit of the NCUA's Enterprise Risk Management (ERM) Risk Profiles

OMB Circular A-123 provides that ERM is an agency-wide approach to addressing the full spectrum of the agency's external and internal risks by understanding the combined impact of risks as an interrelated portfolio, rather than addressing risks only within silos. ERM provides an enterprise-wide, strategically aligned portfolio view of organizational challenges that provides better insight into how to most effectively prioritize resource allocations to ensure successful mission delivery. While agencies cannot respond to all risks related to achieving strategic



April 1, 2025 - September 30, 2025

objectives and performance goals, they must identify, measure, and assess risks related to mission delivery.

The NCUA is exposed to a variety of risks related to its mission and operations, including in its regulation and supervision of over 4,000 federally insured credit unions. Through its ERM program, the agency expects to manage risks to achieving its mission and maximizing opportunities. ERM should address the full spectrum of risks related to achieving the NCUA's strategic objectives and provide agency leadership a complete view of risk to help inform decision making.

We are conducting this self-initiated audit to determine whether the NCUA adequately established, maintained, and used risk profiles to address enterprise-level risks.

Material Loss Reviews (MLR)

The Federal Credit Union Act requires the OIG to conduct an MLR of an insured credit union if the loss to the Share Insurance Fund exceeds \$25 million and an amount equal to 10 percent of the total assets of the credit union at the time in which the NCUA Board initiated assistance or was appointed liquidating agent pursuant to the Act. When losses exceed this materiality threshold, we review the loss to: (1) determine the cause(s) of the credit union's failure and the resulting loss to the Share Insurance Fund; and (2) assess the NCUA's supervision of the credit union. During this reporting period, the Share Insurance Fund had no losses exceeding the materiality threshold.

Report on Credit Union Non-Material Losses

For any loss to the Share Insurance Fund that does not meet the threshold, the Federal Credit Union Act requires the OIG to conduct a limited-scope review to determine whether unusual circumstances exist related to the loss that would warrant conducting a full-scope MLR. For the current reporting period, the Share Insurance Fund incurred a loss below the threshold due to six failed credit unions. We conducted a limited-scope review on the failed credit unions. For each limited-scope review, we performed procedures that included: (1) obtaining and analyzing the regulator's supervisory memoranda and other pertinent documents; (2) preparing a schedule of CAMELS ratings assigned to the institution through full scope or other examinations during the 5 years preceding the failure; (3) conducting interviews as needed; (4) inquiring about any investigative actions taken, planned, or considered involving credit union officials or others; and (5) analyzing supervisory history and other review methods. Based on our reviews, we determined none of the losses involved unusual circumstances warranting conducting a full-



April 1, 2025 - September 30, 2025

scope MLR. The following chart provides details on the six credit unions and our decision not to conduct further work.

OIG'S DECISION REGARDING LOSSES LESS THAN \$25 MILLION					
<u>OIG Decision</u>	<u>Credit Union</u>	<u>Region</u>	<u>Liquidation Date</u>	<u>Est. Loss to Share Insurance Fund</u>	<u>Grounds for Liquidation or Appointment</u>
Terminate	Unilever Federal Credit Union (Unilever)	Eastern	4/30/2025	\$8,440,000	Unilever was involuntarily liquidated due to fraud. Two credit union employees hid borrowings and used them to conceal their fraudulent activity and mask the credit union's true liquidity position.
Terminate	Eastern Kentucky Federal Credit Union (Eastern Kentucky)	Southern	6/5/2025	\$1,471,759	Eastern Kentucky merged with Commonwealth Federal Credit Union with a cash assistance. Eastern Kentucky failed due to management's lack of follow-up and detailed knowledge of its loan portfolio.
Terminate	Soul Community Federal Credit Union (Soul Community)	Southern	6/20/2025	\$91,425	Soul Community was involuntarily liquidated due to insolvency, violations of the Federal Credit Union Act and NCUA rules and regulations, and because it operated in an unsafe and unsound manner.
Terminate	Butler Heritage Federal Credit Union (Butler Heritage)	Southern	6/30/2025	\$192,525	Butler Heritage was liquidated with a purchase and assumption by Cincinnati Ohio Police Federal Credit Union. Butler Heritage failed due to mismanagement that resulted in continued financial losses and failure to comply with record keeping, Bank Secrecy Act, and information technology requirements.



April 1, 2025 - September 30, 2025

Terminate	Aldersgate Federal Credit Union (Aldersgate)	Western	7/1/2025	\$7,975,902	Aldersgate was involuntarily liquidated due to insolvency related to management's fraudulent activities involving multiple loans and share accounts.
Terminate	Members First of Maryland Federal Credit Union (Members First)	Eastern	8/29/2025	\$230,520	Members First was liquidated with a purchase and assumption by Aberdeen Proving Ground Federal Credit Union. Members First failed because of pervasive record weaknesses, deficient earnings, elevated operating expenses, and declining net worth.



April 1, 2025 - September 30, 2025

Significant Recommendations on Which Corrective Action Has Not Been Completed

Following is a list of OIG reports with significant unimplemented recommendations as of September 30, 2025. NCUA management previously agreed to implement corrective actions but had not completed those actions. This information was supplied by the NCUA's Office of the Executive Director and is monitored within the OIG's report recommendation tracking system.

Open Significant Recommendations and Brief Summary

1. **OIG-24-01** *Audit of NCUA's Cloud Computing Services*, issued February 12, 2024, recommendation #1. Finalize and implement a comprehensive formalized enterprise-wide cloud computing strategy that, at minimum, addresses the following:

- Alignment with federal guidance and directives such as Cloud Smart and Executive Order 14028.
- Prioritization of the use of FedRAMP-authorized systems.
- Identification of workforce requirements needed to support cloud procurement, implementation, and risk management.
- Management of risks related to the use of cloud computing services such as secure cloud architecture, data governance, and incident management processes.

Status: Open. Management indicated that an evaluation and implementation of corresponding changes will be completed by December 31, 2025.

2. **OIG-24-09** *Audit of the NCUA's Federal Chartering Process*, issued November 6, 2024, recommendation #1. Develop a centralized system and institute a phone log system to modernize and streamline the chartering application process.

Status: Open. Management stated that the 2025-2026 Staff Draft Budget includes an initial \$1 million capital investment for the development of requirements for a multi-year process automation project for field of membership and new charter requests.

3. **OIG-25-08** *NCUA Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2025*, issued August 20, 2025, recommendation #4. Implement baseline compliance monitoring for routers, switches, and firewalls on the NCUA network. This includes documenting deviations from the configuration baselines and providing business justifications for these deviations.



April 1, 2025 - September 30, 2025

Status: Open. Management indicated that baseline compliance for monitoring for routers and switches has been implemented. The agency will extend this monitoring to include firewalls no later than March 31, 2026.

Summary of Audit Reports Over 6 Months Old with Unimplemented Recommendations

Following are summaries of 7 OIG audit reports over 6 months old that have a total of 11 unimplemented recommendations, including any associated cost savings, as of September 30, 2025. For each of these reports, NCUA management agreed to implement corrective actions but had not completed those actions. The OIG monitors this information within its report recommendation tracking system.

Report Summary and Unimplemented Recommendations

1. **OIG-21-09** *NCUA Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2021*, issued November 22, 2021, Number of Open Recommendations Remaining: 1, Potential Cost Savings: \$0

The OIG made the following recommendation to assist the agency in improving the effectiveness of its information security and its privacy programs and practices.

Unimplemented Recommendation

Recommendation #1—Review the Supply Chain Risk Management (SCRM) National Institute of Standards and Technology (NIST) guidance and update the SCRM plan, policies, and procedures to fully address supply chain risk management controls and practices.

2. **OIG-23-05** *National Credit Union Administration Cybersecurity Audit*, issued May 2, 2023, Number of Open Recommendations Remaining: 1, Potential Cost Savings: \$0.

The OIG made the following recommendation to assist the agency in improving the effectiveness of cybersecurity controls related to its firewall and audit logging security technologies.



April 1, 2025 - September 30, 2025

Unimplemented Recommendation

Recommendation #4—Complete implementation of OMB M-21-31 to achieve past due Event Logging 1 and 2 maturity levels and to meet the Event Logging 3 maturity due by August 27, 2023.

3. **OIG-24-01** *Audit of NCUA's Cloud Computing Services*, issued February 12, 2024, Number of Open Recommendations Remaining: 2, Potential Cost Savings: \$0

The OIG made the following recommendations to assist the agency in improving its operational and security risks of implemented cloud computing services.

Unimplemented Recommendations

Recommendation #1—Finalize and implement a comprehensive formalized enterprise-wide cloud computing strategy that, at minimum, addresses the following:

- Alignment with federal guidance and directives such as Cloud Smart and Executive Order 14028.
- Prioritization of the use of FedRAMP-authorized systems.
- Identification of workforce requirements needed to support cloud procurement, implementation, and risk management.
- Management of risks related to the use of cloud computing services such as secure cloud architecture, data governance, and incident management processes.

Recommendation #2— Develop and implement policies, procedures, and standards that are consistent with the NCUA's cloud computing strategy and address, at minimum, the following:

- Coordination, identification, and clarification of responsibilities and processes across all stakeholders for IT service contract reviews, service-level agreements alignment and monitoring, and cloud service incident management.
- Specific criterion for the prioritization, selection, and use of cloud computing services.
- Periodic review of contract clauses included for cloud computing services to confirm documentation supporting security requirements are clearly identified to the vendor and security and operational risks are appropriately managed.

4. **OIG-24-06** *Audit of NCUA's Bank Secrecy Act Enforcement*, issued May 30, 2024, Number of Open Recommendations Remaining: 1, Potential Cost Savings: \$0



April 1, 2025 - September 30, 2025

The OIG made the following recommendation to assist the agency in improving its enforcement of the Bank Secrecy Act.

Unimplemented Recommendation

Recommendation #4—Revise the NCUA’s Enforcement Manual to include current policies, procedures, and responsibilities for the NCUA’s formal enforcement actions and ensure its content is consistent with other NCUA policies. Regularly review this guidance for continued relevance and effectiveness in achieving the agency’s objectives.

5. **OIG-24-08** *NCUA Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2014*, issued September 12, 2024, Number of Open Recommendations Remaining: 2, Potential Cost Savings: \$0

The OIG made the following recommendations to assist the agency in improving the effectiveness of its information security and privacy programs and practices.

Unimplemented Recommendations

Recommendation #1—Conduct refresher training for the property custodians regarding documenting and maintaining asset management system records in accordance with NCUA policy and procedures.

Recommendation #2—Update the accountable property policy to implement a process for the property management officer to complete a periodic review of the IT asset inventory to validate that the inventory is documented and maintained in accordance with NCUA policy and procedures.

6. **OIG-24-09** *Audit of the NCUA’s Federal Chartering Process*, issued November 6, 2024, Number of Open Recommendations Remaining: 3, Potential Cost Savings: \$0

The OIG made the following recommendations to assist the agency in improving its credit union chartering process.

Unimplemented Recommendations

Recommendation #1—Develop a centralized system and institute a phone log system to modernize and streamline the chartering application process.

Recommendation #2—Quantify and clarify the deferral process for organizing groups by establishing clear guidelines and milestones to ensure enhanced transparency and understanding.



April 1, 2025 - September 30, 2025

Recommendation #3—Post detailed information about the NCUA’s charter deferral process on the agency’s website to clearly communicate expectations and provide organizing groups with a transparent and comprehensive understanding of deferrals within the charter application process.

7. **OIG-25-01** *Audit of the NCUA’s Compliance with its Examiner-in-Charge Rotation Policies and Procedures*, issued February 6, 2025, Number of Open Recommendations Remaining: 1, Potential Cost Savings: \$0

The OIG made the following recommendation to assist the agency in improving its examiner-in-charge rotation policies and procedures.

Unimplemented Recommendation

Recommendation #1—Ensure managers involved in the examination scheduling program adhere to examiner-in-charge rotation limits requirements to ensure timely examiner-in-charge rotation in accordance with the National Supervision Policy Manual.

Recommendations for Corrective Action Made During the Reporting Period

During the reporting period, the OIG issued the following 2 audit reports with a total of 18 recommendations for corrective action to improve the effectiveness of the NCUA’s operations.

- OIG-25-07** *Audit of the NCUA’s Cyber Threat Information Sharing*, issued June 9, 2025, Number of Open Recommendations Remaining: 7, Potential Cost Savings: \$0

Recommendation #1—Develop and finalize policies and procedures that address cyber threat information sharing.

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.

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.

Recommendation #4—Update and document incident reporting triage protocols to provide consistent and useable data in the Cyber Incidents for (b) (7)(E) (b) (7)(E).



April 1, 2025 - September 30, 2025

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

Recommendation #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.³

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.

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

OIG-25-08 *NCUA Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2024*, issued August 20, 2025, Number of Open Recommendations Remaining: 10, Potential Cost Savings: \$0

Recommendation #1— Document policies and procedures for developing and maintaining current and target cybersecurity profiles that include, at a minimum, consideration of the NCUA’s mission objectives, threat landscape, and resources (including personnel) and constraints.

Recommendation #2—Create and maintain current and target cybersecurity profiles—including a gap analysis that identifies differences between the current and target state—that consider anticipated changes in the NCUA’s cybersecurity posture.

Recommendation #3— Update and maintain the comprehensive inventory of data and the corresponding metadata to meet the requirements of the Open Government Data Act and OMB Memorandum M-25-05 by the established September 2026 deadline.

Recommendation #4— Implement baseline compliance monitoring for routers, switches, and firewalls on the NCUA network. This includes documenting deviations from the configuration baselines and providing business justifications for these deviations.

Recommendation #5 — Improve processes to ensure that the NCUA remediates workstation vulnerabilities within agency-required timelines, including monitoring for

³ Recommendation has been closed as of September 30, 2025.



April 1, 2025 - September 30, 2025

workstations that have been disconnected from the network for an extended period of time.

Recommendation #6— Develop and implement procedures to remediate vulnerabilities for the (b) (7)(E) within NCUA timeline requirements that fall outside of the (b) (7)(E) monthly patching schedule.

Recommendation #7— Coordinate with (b) (7)(E) to upgrade the (b) (7)(E) software or document any risk-based decisions, including compensating controls.

Recommendation #8— Conduct a review of all current (b) (7)(E) privileged user accounts to ensure that the NCUA has documented access requests and approvals for each privileged user account, as required by NCUA policies and procedures.

Recommendation #9— Validate that the NCUA completes quarterly account reviews for the (b) (7)(E) and (b) (7)(E) systems.

Recommendation #10 — Implement automatic disabling of privileged (b) (7)(E) user accounts upon 30 days of inactivity or document any risk-based decisions, including compensating controls.



April 1, 2025 - September 30, 2025

Peer Reviews

Government Auditing Standards require audit organizations that perform audits and attestation engagements of federal government programs and operations undergo an external peer review every 3 years. The objectives of an external peer review include a review of an audit organization's system of quality control to determine the suitability of its design and whether the audit organization is in compliance with the quality control system so as to provide reasonable assurance the audit organization conforms to applicable professional standards.

External Peer Review of the NCUA OIG, Office of Audit

During this reporting period, the Smithsonian OIG completed our most recent peer review on March 27, 2025, for the 3-year period ending September 30, 2024. The Smithsonian OIG issued its report entitled System Review Report and rendered the opinion that the system of quality control for the OIG, Office of Audit, was suitably designed and complied with, thus providing reasonable assurance the system of controls conformed with applicable professional standards in all material respects. As a result, we received a peer rating of Pass. See Appendix A for a copy of the System Review Report.

External Peer Review of the Library of Congress OIG, Office of Audit

During this reporting period, we were conducting a peer review of the Library of Congress OIG, but our review was suspended until the next reporting period. The last peer review we completed was of the National Labor Relations Board (NLRB) OIG on November 17, 2020. We issued an external peer review report for the audit function of the NLRB OIG for the 3-year period ending September 30, 2020. The NLRB received a rating of Pass and has no outstanding recommendations related to the peer review report.



April 1, 2025 - September 30, 2025

Investigative Activity

In accordance with professional standards and guidelines established by the U.S. Department of Justice and the Council of the Inspectors General on Integrity and Efficiency (CIGIE), the OIG's Office of Investigations (OI) conducts investigations of criminal, civil, and administrative wrongdoing involving the agency's programs, operations, and personnel. Our investigative mission is to fight fraud, waste, and abuse while promoting efficiency and economy within the NCUA and its programs and operations. In this regard, we investigate allegations of misconduct by NCUA employees, former employees, applicants, and contractors. Investigations examine possible violations of applicable federal laws and regulations as well as NCUA-specific policies.

We receive allegations through our electronic hotline form, email, phone, mail, and in person from NCUA and contractor personnel. We also receive complaints from credit union officials and their members regarding NCUA programs, employees, and contractors. We examine these complaints and determine if there is any indication of misconduct or wrongdoing by an NCUA employee or contractor. If not, we refer the complaint to the NCUA's Office of Consumer Financial Protection (OCFP), the Office of General Counsel, or the appropriate regional office for response, or close the matter if contact with those offices indicates that the matter already was appropriately handled. Harassment allegations are addressed by the NCUA's Office of Ethics Counsel and the Office of Minority and Women Inclusion (for EEO complaints).

During this reporting period, OI continued to work on five investigations that we opened during a prior period. As the table below indicates, we referred two investigative subjects for prosecution during the reporting period.

Investigative Activity/Reports Issued During the Reporting Period	Total Number
(A) Investigative reports issued during the reporting period	0
(B) Persons referred to the Department of Justice for criminal prosecution during the reporting period	2
(C) Persons referred to state and local prosecuting authorities for criminal prosecution during the reporting period	0
(D) Indictments and criminal information during the reporting period that resulted from any prior referral to prosecuting authorities	0



April 1, 2025 - September 30, 2025

Regarding the information provided in the table above, OI maintains a manual case tracking system. If investigative allegations involve a named suspect, then cases are designated and tracked by subject name. Cases referred to federal, state, or local prosecuting authorities for criminal prosecution are also designated, referred, and tracked by subject name, if known. In cases where the subject is unknown, OI uses a subject matter title to designate, track, and, as appropriate, refer cases.

Investigations

OI did not close any investigations involving a senior government employee during the reporting period.

Whistleblower Retaliation

We did not receive any complaints of whistleblower retaliation during the reporting period.

Attempts to Interfere with IG Independence

There were no attempts on the part of management to interfere with IG independence, including restricting communications between the OIG and Congress or using budgetary constraints designed to limit the capabilities of the OIG. Moreover, there have been no incidents where the NCUA resisted or objected to OIG oversight activities. There have also been no restrictions or delays in our access to agency information.

Administrative False Claims Act

The OIG did not investigate any cases under the Administrative False Claims Act and did not make any reports to the NCUA under the Act.

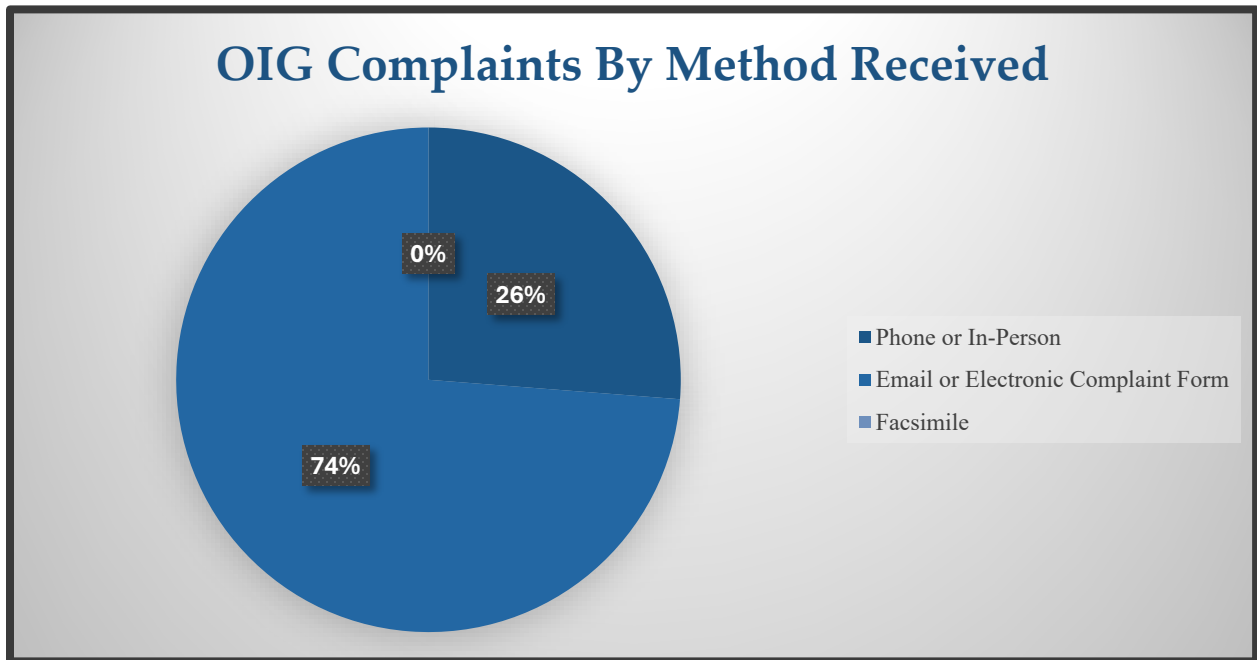
OIG Hotline and FOIA Requests

The OIG maintains a 24-hour toll-free hotline to enable employees and citizens to call in and provide information about suspected fraud, waste, and abuse, or mismanagement involving agency programs or operations and an online hotline portal on the OIG's webpage. Additionally, the OIG receives complaints from an off-site post office box, electronic mail, facsimile messages, and in person. An electronic hotline complaint form is located on the NCUA intranet for confidential employee and contractor communication with the OIG. Our Office Manager, under the direction of the Director of Investigations, administers the OIG hotline program.



April 1, 2025 - September 30, 2025

During this 6-month period, we processed 61 hotline complaints. This number does not reflect consumers seeking assistance with problems encountered with their respective credit unions. We referred most of those complaints to the OCFP's Consumer Assistance Center for action. OIG also responded to 32 Freedom of Information Act requests during the reporting period.



Complaints by Method Received	Number
Mail or Facsimile	0
Phone or In-Person	16
Email or Electronic Hotline Complaint Form	45
Total:	61



April 1, 2025 - September 30, 2025

Reviews of Legislation, Regulations, and Policies

Section 4(a) of the Inspector General Act requires the Inspector General to review existing and proposed legislation and regulations relating to the programs and operations of the NCUA and to make recommendations concerning their impact. OIG reviewed the legislation and NCUA regulations listed below. In addition, the OIG reviewed executive orders and related guidance.

List of Legislation and Regulations Reviewed

Legislation	Title
Pub. L. 119-21	One Big Beautiful Bill Act
Pub. L. 119-27	GENIUS Act
Regulations	Title
12 C.F.R. Parts 745 and 701	Simplification of Share Insurance and Succession Planning
N/A	Voluntary Review of Regulations Contemplated by Economic Growth and Regulatory Paperwork Reduction Act



April 1, 2025 - September 30, 2025

TABLE I : ISSUED REPORTS WITH QUESTIONED COSTS

Issued Reports with Questioned Costs	Number of Reports	Questioned Costs	Unsupported Costs
(A) For which no management decision had been made by the start of the reporting period.	0	\$0	\$0
(B) Which were issued during the reporting period.	0	\$0	\$0
Subtotals (A + B)	0	\$0	\$0
(C) For which management decision was made during the reporting period.	0	\$0	\$0
(i) Dollar value of disallowed costs	0	\$0	\$0
(ii) Dollar value of costs not allowed	0	\$0	\$0
(D) For which no management decision has been made by the end of the reporting period.	0	\$0	\$0
(E) Reports for which no management decision was made within 6 months of issuance.	0	\$0	\$0

Questioned costs means a cost the OIG has questioned because of alleged violations of laws, regulations, contracts, or other agreements; a finding at the time of the audit that such cost is not supported by adequate documentation; or a finding that the expenditure of funds for the intended purpose is unnecessary or unreasonable.

Unsupported costs (included in "Questioned Costs") means a cost the OIG has questioned because it was not supported by adequate documentation.



April 1, 2025 - September 30, 2025

TABLE II: ISSUED REPORTS WITH RECOMMENDATIONS THAT FUNDS BE PUT TO BETTER USE

Issued Reports with Recommendations That Funds Be Put To Better Use	Number of Reports	Dollar Value
(A) For which no management decision had been made by the start of the reporting period.	0	\$0
(B) Which were issued during the reporting period.	0	\$0
Subtotals (A + B)	0	\$0
(C) For which management decision was made during the reporting period.	0	\$0
(i) Dollar value of recommendations agreed to by management.	0	\$0
(ii) Dollar value of recommendations not agreed to by management.	0	\$0
(D) For which no management decision was made by the end of the reporting period.	0	\$0
(E) Reports for which no management decision was made within 6 months of issuance.	0	\$0

Recommendation that funds be put to better use are OIG recommendations that funds could be used more efficiently if management took actions to reduce outlays, de-obligate funds from programs/operations, avoid unnecessary expenditures noted in pre-award reviews of contracts, or any other specifically identified savings.

TABLE III: SUMMARY OF OIG AUDIT ACTIVITY DURING THE REPORTING PERIOD

Audit Reports Issued	Title	Date Issued
OIG-25-07	Audit of the NCUA's Cyber Threat Information Sharing	6/9/2025
OIG-25-08	FY 2025 Independent Evaluation of the NCUA's Compliance with the Federal Information Security Modernization Act of 2014 (FISMA)	8/20/2025

TABLE IV: SUMMARY OF OIG AUDITS IN PROGRESS (AS OF SEPTEMBER 30, 2025)

Title
Audit of the NCUA's Information Technology Asset Sanitization Process
Audit of the NCUA's Travel Card Program
Audit of the NCUA's Field Employees' Duty Station and Work Activities
Audit of the NCUA's Enterprise Risk Management Risk Profiles



April 1, 2025 - September 30, 2025

INDEX OF REPORTING REQUIREMENTS OF THE INSPECTOR GENERAL ACT, 5 U.S.C. §§ 401-424		
Section	Reporting Requirement	Page
404(a)(2)	Review of legislation and regulations	26
405(b)(1)	Significant problems, abuses, and deficiencies	15
405(b)(2)	Recommendations for corrective action made during the reporting period	19
405(b)(3)	Significant recommendations on which corrective action has not been completed	15
405(b)(4)	Matters referred to prosecutive authorities	23
405(b)(5)	Summary of each report made to the agency head when instances where agency refused or failed to provide requested information	N/A
405(b)(6)	List of audit reports issued during the reporting period	28
405(b)(7)	Summary of significant reports issued during the reporting period	N/A
405(b)(8)	Statistical table on audit reports with questioned costs	27
405(b)(9)	Statistical table on audit reports with recommendations that funds be put to better use	28
405(b)(10)(A)	Summary of each audit report over six months old for which no management decision has been made	N/A
405(b)(10)(B)	Summary of each audit report over six months old for which no management comment was returned within 60 days	N/A
405(b)(10)(C)	Summary of each audit report over six months old for which there are unimplemented recommendations	16



April 1, 2025 - September 30, 2025

INDEX OF REPORTING REQUIREMENTS OF THE INSPECTOR GENERAL ACT, 5 U.S.C. §§ 401-424		
Section	Reporting Requirement	Page
405(b)(11)	Significant revised management decisions	N/A
405(b)(12)	Significant management decisions with which the OIG disagreed	N/A
405(b)(14)(A)(B)	Results of any peer review conducted during the reporting period, or if no peer review was conducted, a statement identifying the date of last peer review	22
405(b)(15)(16)	Peer reviews conducted by another OIG during the reporting period, and any outstanding recommendations from any current or prior peer review	31
405(b)(17)	Statistical table on investigative reports issued during the reporting period	23
405(b)(18)	Description of metrics used for developing the investigative report statistical table	24
405(b)(19)	Investigations conducted involving a senior Government employee	N/A
405(b)(20)	Detailed description of any instances of whistleblower retaliation	N/A
405(b)(21)	Detailed description of any attempt by the agency to interfere with the independence of the Office	N/A
405(b)(22)(A)	Detailed description of any inspection, evaluation, and audit that was closed and was not disclosed to the public	N/A
405(b)(22)(B)	Detailed description of any investigation involving a senior Government employee that was closed and was not disclosed to the public	N/A



April 1, 2025 - September 30, 2025

Appendix A

System Review Report

Docusign Envelope ID: CF1AC70E-68CA-4DB0-A880-7016536D252B

OFFICE OF THE INSPECTOR GENERAL



System Review Report

March 27, 2025

James W. Hagen
Inspector General
National Credit Union Administration
1775 Duke Street
Alexandria, VA 22314

Dear Mr. Hagen:

We have reviewed the system of quality control for the audit organization of the National Credit Union Administration Office of the Inspector General (NCUA OIG) in effect for the year ending September 30, 2024. A system of quality control encompasses NCUA OIG's organizational structure and the policies adopted and procedures established to provide reasonable assurance of conforming in all material respects with *Government Auditing Standards* and applicable legal and regulatory requirements.¹ The elements of quality control are described in *Government Auditing Standards*.

In our opinion, the system of quality control for the audit organization of NCUA OIG in effect for the year ending September 30, 2024, has been suitably designed to provide NCUA OIG with reasonable assurance of performing and reporting in conformity with applicable professional standards and applicable legal and regulatory requirements in all material respects.

Audit organizations can receive a rating of pass, pass with deficiencies, or fail. NCUA OIG has received an External Peer Review rating of pass.

Monitoring of GAGAS Engagements Performed by Independent Public Accountants

In addition to reviewing its system of quality control to ensure adherence with *Government Auditing Standards*, we applied certain limited procedures in accordance with guidance established by the Council of the Inspectors General on Integrity and Efficiency (CIGIE) related to NCUA OIG's monitoring of engagements conducted in accordance with generally accepted government auditing standards (GAGAS engagements) by independent public accountants (IPAs) under contract where the IPA served as the auditor. It should be noted that monitoring of GAGAS engagements performed by IPAs is not an audit and, therefore, is not subject to the requirements of *Government Auditing Standards*. The purpose of our limited procedures was to determine whether NCUA OIG had controls to ensure IPAs performed contracted work in accordance with professional standards. Our objective was not to express an opinion; accordingly, we do not express an opinion on NCUA OIG's monitoring of work performed by IPAs.

¹ *Government Auditing Standards*, 2018 Revision (July 2018).

MRC 524
PO Box 37012
Washington DC 20013-7012
202.633.7050 Telephone
202.633.7079 Fax
www.si.edu/oig



April 1, 2025 - September 30, 2025

DocuSign Envelope ID: CF1AC70E-68CA-4DB0-A880-7016536D252B

Letter of Comment

We have issued a letter dated March 27, 2025, that sets forth a finding that was not considered to be of sufficient significance to affect our opinion expressed in this report. We also made a comment related to NCUA OIG's monitoring of GAGAS engagements performed by IPAs, which we included in the above-referenced letter.

Basis of Opinion

Our review was conducted in accordance with *Government Auditing Standards* and CIGIE's *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General*.²

During our review, we interviewed NCUA OIG personnel and obtained an understanding of the nature of NCUA OIG audit organization, and the design of NCUA OIG's system of quality control sufficient to assess the risks implicit in its audit function. Based on our assessments, we selected GAGAS engagements and administrative files to test for conformity with professional standards and compliance with NCUA OIG's system of quality control. The GAGAS engagements selected represented a reasonable cross-section of NCUA OIG's audit organization, with an emphasis on higher-risk engagements.

In performing our review, we obtained an understanding of the system of quality control for the NCUA OIG audit organization. In addition, we tested compliance with NCUA OIG's quality control policies and procedures to the extent we considered appropriate. These tests covered the application of NCUA OIG's policies and procedures on selected GAGAS engagements. Our review was based on selected tests; therefore, it would not necessarily detect all weaknesses in the system of quality control or all instances of noncompliance with it.

Prior to concluding the peer review, we reassessed the adequacy of the scope of the peer review procedures and met with NCUA OIG management to discuss the results of our review. We believe that the procedures we performed provide a reasonable basis for our opinion. Enclosure 1 to this report identifies the NCUA OIG engagements we reviewed.

Responsibilities and Limitation

NCUA OIG is responsible for establishing and maintaining a system of quality control designed to provide NCUA OIG with reasonable assurance that the organization and its personnel comply in all material respects with professional standards and applicable legal and regulatory requirements. Our responsibility is to express an opinion on the design of the system of quality control and NCUA OIG's compliance based on our review.

² CIGIE, *Guide for Conducting Peer Reviews of Audit Organizations of Federal Offices of Inspector General* (March 2020).



April 1, 2025 - September 30, 2025

Docusign Envelope ID: CF1AC70E-68CA-4DB0-A880-7016536D252B

There are inherent limitations in the effectiveness of any system of quality control; therefore, noncompliance with the system of quality control may occur and may not be detected. Projection of any evaluation of a system of quality control to future periods is subject to the risk that the system of quality control may become inadequate because of changes in conditions, or because the degree of compliance with the policies or procedures may deteriorate.

Sincerely yours,

Signed by:

6E3A9C42718646B...
Nicole L. Angarella
Inspector General

Enclosures - 2



April 1, 2025 - September 30, 2025

Docusign Envelope ID: CF1AC70E-68CA-4DB0-A880-7016536D252B

Enclosure 1

Scope and Methodology

We tested compliance with the NCUA OIG audit organization's system of quality control to the extent we considered appropriate. These tests included a review of 4 of 11 engagement reports conducted in accordance with generally accepted government auditing standards (GAGAS) issued from October 1, 2021, through September 30, 2024, as shown in Table 1. We also reviewed the internal quality control reviews performed by NCUA OIG.

Table 1. GAGAS Engagements Performed by NCUA OIG That Were Reviewed

Report Number	Report Date	Report Title
OIG-24-01	February 12, 2024	Audit of the NCUA's Cloud Computing Services
OIG-24-06	May 30, 2024	Audit of the NCUA's Bank Secrecy Act Enforcement Program
OIG-24-07	June 18, 2024	Audit of the NCUA's Examination Hours
OIG-23-06	May 16, 2023	Audit of the NCUA's Contracting Officer's Representative Program

In addition, we reviewed NCUA OIG's monitoring of GAGAS engagements performed by independent public accountants (IPA) where the IPA served as the auditor from October 1, 2021, through September 30, 2024, as shown in Table 2. During the period, NCUA OIG contracted for the audit of its agency's fiscal year 2023 financial statements. NCUA OIG also contracted for other GAGAS engagements that were performed in accordance with *Government Auditing Standards*.

Table 2. NCUA OIG's Monitoring File for Contracted GAGAS Engagement That Was Reviewed

Report Number	Report Date	Report Title
OIG-24-02/03/04/05	February 13, 2024	FY 2023 Financial Statement Audits (SIF, OF, CLF, CDRLF)

We visited NCUA OIG's headquarters located in Alexandria, VA.



April 1, 2025 - September 30, 2025

Docusign Envelope ID: CF1AC70E-68CA-4DB0-A880-7016536D252B



National Credit Union Administration

Enclosure 2

Office of Inspector General

March 26, 2025

Nicole L. Angarella
Inspector General
Smithsonian Office of Inspector General
Washington, D.C. 20013

Subject: System Review Report of the National Credit Union Administration Office of Inspector General Audit Organization

Dear Ms. Angarella:

We appreciate the work conducted by your staff in reviewing the quality control process for the audit function at the National Credit Union Administration Office of Inspector General. We agree with your opinion that the system of quality control for the audit function has been suitably designed and complied with to provide reasonable assurance of performing and reporting in conformity with applicable professional standards and applicable legal and regulatory requirements in all material aspects. We have no additional comments on the final System Review draft report provided. Thank you for your efforts in completing this review.

Sincerely,

A handwritten signature in black ink, appearing to read 'James W. Hagen'.

James W. Hagen
Inspector General

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6350