OIG/JH

SENT BY EMAIL

TO: The Honorable Kyle S. Hauptman, Chairman
The Honorable, Todd M. Harper, Board Member
The Honorable Tanya F. Otsuka, Board Member

FROM: Inspector General James W. Hagen

SUBJ: Top Management and Performance Challenges Facing the National Credit Union Administration for 2025

DATE: February 11, 2025

The Inspector General is required by the Reports Consolidation Act of 2000, 31 U.S.C. § 3516, to provide an annual statement on the top management and performance challenges facing the agency and to briefly assess the agency's progress to address them. We identified the top challenges facing the National Credit Union (NCUA) for 2025 based on our past and ongoing work, our knowledge of the NCUA's programs and operations, and information from the U.S. Government Accountability Office and NCUA management and staff. In determining whether to identify an issue as a challenge, we consider its significance in relation to the NCUA's mission, its susceptibility to fraud, waste, or abuse, and the NCUA's progress in addressing the challenge.

We identified five top challenges facing the NCUA as follows:

1. Managing Interest Rate Risk
2. Managing Credit and Liquidity Risks
3. Cybersecurity – Protecting Systems and Data
4. Risks Posed by Third-Party Service Providers
5. Implementation of Artificial Intelligence (AI)

We believe our identification of top challenges will be beneficial and constructive for policy makers, including the NCUA and Congressional oversight bodies. We further hope that it is informative for the credit union industry regarding the programs and operations at the NCUA and the challenges it faces.

Information on the challenge areas and related Office of Inspector General work products are found in the attachment. If you have any questions, please contact me or Bill Bruns, Deputy Inspector General.

Attachment

cc: Executive Director Larry D. Fazio
Deputy Executive Director (Acting) Towanda A. Brooks
General Counsel Frank S. Kressman
Acting Director, Office of External Affairs and Communications Alfred V. Garesche

INTRODUCTION

Below is a brief overview of the NCUA's organizational structure, its mission, and vision, as well as details on each of the top management challenges my office identified for 2025.

Organizational Structure

The NCUA is an independent federal agency that insures deposits at all federal and most state-chartered credit unions and regulates federally chartered credit unions. A presidentially appointed three-member Board oversees the NCUA's operations by setting policy, approving budgets, and adopting rules.

Agency Strategic Goals

In its 2022-2026 Strategic Plan, the NCUA states that its strategic goals will be to (1) ensure a safe, sound, and viable system of cooperative credit that protects consumers, (2) improve the financial well-being of individuals and communities through access to affordable and equitable financial products and services, and (3) maximize organizational performance to enable mission success.

AGENCY CHALLENGES

Managing Interest Rate Risk

The economic environment is a key determinant of credit union performance. The Federal Reserve adjusts the federal funds rate based on economic indicators with the goal of achieving its dual mandate of keeping prices stable and maximizing employment. Despite recent rate cuts, the tightening in U.S. monetary policy over the past 2 years has increased the importance of interest rate risk management at credit unions as higher interest rates continue to expand market risk. Job and wage growth and low unemployment supported consumer spending throughout the year, with spending growth strengthening in the second half of 2024 as inflation continued to move lower.

High levels of interest rate risk can increase a credit union's liquidity risks, contribute to asset quality deterioration and capital erosion, and put pressure on earnings. As stated in our previous management challenges statement, credit unions must continue to be prudent and proactive in managing interest rate risk and the related risks to capital, asset quality, earnings, and liquidity. This is particularly the case for those credit unions whose assets are concentrated in fixed-rate long term mortgages that were originated when interest rates were at record lows. Since April 2022, the NCUA has been using the revised CAMELS Rating System that includes the S component (Sensitivity to Market Risk), which I believe has helped the agency focus on these risks to ensure they remain within safe and sound policy limits.

For 2025, credit unions' ability to manage and mitigate interest rate risk and the NCUA's continued focus to ensure this risk is monitored and measured will continue to be extremely important. Therefore, the NCUA must continue to analyze the S component to determine whether credit unions are proactively managing their interest rate risk and the related risks to capital, asset quality, earnings, and liquidity to ensure their overall level of interest exposure is properly measured and controlled.

Managing Credit Risk and Liquidity Risk

The Congressional Budget Office (CBO) projects that the growth of real gross domestic product (GDP) will decrease from an estimated 2.3 percent in calendar year 2024 to 1.9 percent in 2025. Since June 2024, when the CBO published its updated economic forecast, projections of the average growth rate of GDP over the 2024–2026 period have changed little. The CBO lowered its forecast of employment growth over that period and expects inflation to be slightly higher, on average, in 2025.[1] Slowing employment growth and moderately higher inflation could cause challenges for credit unions, such as reduced loan demand and higher credit risk. The changing interest rate environment could also affect credit union performance. In 2023, rising short-term interest rates put pressure on credit unions to raise deposit rates to avoid deposit attrition. The decline in short-term interest rates in late 2024 should relieve pressure on credit union funding costs and liquidity, and many experts believe long-term rates also will decline, which could put downward pressure on credit union loan rates.

The NCUA has taken actions to address credit and liquidity risks. Agency regulations contain credit union contingency funding plan expectations scaled according to a credit union's assets. In July 2023, the NCUA issued Letter to Credit Unions 23-CU-06, *Importance of Contingency Funding Plans*, and added an addendum to the 2010 *Interagency Policy Statement on Funding and Liquidity Risk Management*, both of which continue to reinforce the need for credit unions to adjust to changing market conditions. It is imperative the NCUA continues to examine credit unions under this framework in 2025. Also, audit report #OIG-15-11 recommended that the NCUA modify the "L" (Liquidity) in the CAMELS rating system to not only evaluate credit unions' policies, procedures, and risk limits, but also credit unions' current and prospective sources of liquidity, the adequacy of its liquidity risk management framework relative to its size, complexity, and risk profile compared to funding needs. The NCUA has been reviewing these expanded areas of the "L" component since April 2022.

Cybersecurity and IT Governance – Protecting Systems and Data

As stated in our previous management challenges statement, cybersecurity risks continue to remain a significant, persistent, and ever-changing threat to the financial sector. Credit unions' growing reliance on increasingly complex technology-related operating environments exposes the credit union system to escalating cyberattacks. Cyberattacks can affect the safety and soundness of credit unions and lead to their failure, thus causing losses to the NCUA's Share Insurance Fund. The prevalence of malware, ransomware, distributed denial of service attacks,

[1] The Budget and Economic Outlook: 2025 to 2035 | Congressional Budget Office

and other forms of cyberattacks are causing challenges at credit unions of all sizes, which will require credit unions to continually evolve and adapt to counter these threats effectively. These trends are likely to continue, and even accelerate, in the years ahead.

For 2025, the NCUA must continue to prioritize this area as a key examination focus and continue to assess whether credit unions have implemented robust information security programs to safeguard both members and the credit unions themselves. The NCUA must remain focused on advancing consistency, transparency, and accountability within its information technology and cybersecurity examination program. To help the agency provide credit unions the capability to conduct a maturity assessment aligned with the Federal Financial Institutions Examination Council Cybersecurity Assessment Tool, the NCUA must continue to improve and enhance its Information Security Examination (ISE) program. Building off its Automated Cybersecurity Evaluation Tool (ACET) application, which allows institutions, regardless of size, to voluntarily maintain a high level of vigilance and ability to respond to evolving cybersecurity threats by measuring their cybersecurity preparedness and identifying opportunities for improvement, the ISE program will provide examiners with standardized review steps that should facilitate advanced data collection and analysis. It is important that the NCUA continues to encourage credit unions to access the NCUA's Cybersecurity Resources webpage for cybersecurity information and resources. These resources provide valuable insights and guidance to help credit unions strengthen their cybersecurity stance and stay abreast of the latest developments.

Last year's management challenges statement highlighted the growing frequency and severity of cyber incidents within the financial services industry, which unfortunately still holds true. Since September 2023, the NCUA's Cyber Incident Notification Reporting Rule has required federally insured credit unions to notify the NCUA within 72 hours after they reasonably believe that a reportable cyber incident has occurred, including if a third-party provider experiences a cyber incident affecting the credit union. In the OIG's 2025 Annual Work Plan, my office has two audits planned to address cybersecurity-related issues. One will assess whether the new reporting rule is working as intended and the other, which will soon be issued to the NCUA Board and management, will report our findings and recommendations on the agency's efforts to share threat information.

In addition, pursuant to the Federal Information Modernization Act of 2014 (FISMA), Pub. L. No. 113-283, we engaged a contractor to annually evaluate the NCUA's implementation of FISMA information security requirements and the effectiveness of the agency's information security program on a maturity model scale. On September 12, 2024, we issued the contractor's FISMA report titled, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2024*, #OIG-24-08. The contractor determined the NCUA implemented an effective information security program by achieving an overall Level 4 - Managed and Measurable maturity level, complied with FISMA, and substantially complied with agency information security and privacy policies and procedures. As stated in its 2022-2026 Strategic Plan, NCUA management recognizes that cybersecurity threats and other technology-related issues continue to concern the agency as increasingly sophisticated cyberattacks pose a significant threat to credit unions, financial regulators, and the broader financial services sector.

Risk Posed by Third-Party Vendors and Credit Union Service Organizations

Even with implementation of the Cyber Incident Notification Reporting Rule, the credit union system remains vulnerable in part because the NCUA lacks vendor oversight authority. Without this authority, the NCUA cannot accurately assess the actual risk present in the credit union system or determine if the risk-mitigation strategies of credit union service organizations and third-party vendors, which provide much of the industry's information technology infrastructure, are adequate and can effectively protect the credit union system from potential attacks. This regulatory blind spot leaves thousands of credit unions, millions of credit union members, and billions of dollars in assets potentially exposed to unnecessary risks. To address this, the NCUA continues to request authority comparable to its counterparts on the Federal Financial Institutions Examination Council (FFIEC) to examine credit union service organizations and third-party vendors.

Although Congress provided the NCUA vendor oversight authority in 1998 in response to concerns about the Y2K changeover, that authority expired in 2002. Since then, the OIG, the Financial Stability Oversight Council, and the Government Accountability Office have each recommended that this authority be restored.

Currently, the NCUA may only examine credit union service organizations and third-party vendors with their permission, and they at times have declined these requests. Further, vendors can reject the NCUA's recommendations to implement appropriate corrective actions to mitigate identified risks. This lack of authority stands in stark contrast to the authority of NCUA's counterparts on the FFIEC.

Activities that are fundamental to the credit union mission, such as loan origination, lending services, Bank Secrecy Act/anti-money laundering compliance, and financial management, are being outsourced to entities that are outside of the NCUA's regulatory oversight. In addition, credit unions are increasingly using third-party vendors to provide technological services, including information security and mobile and online banking. Member data is stored on vendors' servers.

As stated in previous management challenges statements, my office issued audit report #OIG-20-07 on NCUA's lack of vendor authority. In that audit, we determined the NCUA needs authority over credit union service organizations and vendors to effectively identify and reduce the risks vendor relationships pose to credit unions to protect the Share Insurance Fund. The audit concluded that despite the NCUA's ability to conduct limited credit union service organization reviews, there is currently nothing in the Federal Credit Union Act that provides the NCUA with the authority to supervise credit union service organizations to hold them accountable for unsafe and unsound practices that have direct and lasting impact on the credit unions they serve. In addition, the audit determined the lack of statutory vendor oversight and regulatory enforcement authority hinders the NCUA's ability to conduct effective reviews of vendors. As a result, the NCUA's Share Insurance Fund is exposed to risk from credit union service organizations and

vendors that can cause significant financial hardship, or even failure, to the credit unions that use them.

While there are many advantages to using service providers, the concentration of credit union services within credit union service organizations and third-party vendors presents safety and soundness and compliance risk for the credit union industry. The continued transfer of operations to credit union service organizations and vendors lessens the ability of NCUA to accurately assess all the risks present in the credit union system and determine if current risk mitigation strategies are adequate. Audit report #OIG-20-07 confirmed that the NCUA needs comparable authority as its FFIEC counterparts to ensure a safe and sound credit union system.

Implementation of Artificial Intelligence

The NCUA and other government agencies face the challenge of benefiting from the use of artificial intelligence (AI) while also addressing its risks. To reduce costs and improve efficiencies, a growing number of financial firms are using AI for tasks such as fraud prevention, customer service, and credit underwriting. However, the use of AI also introduces potential risks such as safety and soundness and consumer compliance risk. The Federal Stability Oversight Counsel, of which the NCUA Chairman is a member, recommends monitoring the rapid developments in AI, including generative AI, to ensure that oversight structures keep up with or stay ahead of emerging risks to the financial system while facilitating efficiency and innovation. To support this effort, the Council recommends financial institutions, market participants, and regulatory and supervisory authorities further build expertise and capacity to monitor AI innovation and usage and identify emerging risks. On January 22, 2025, NCUA Chairman Hauptman announced among his priorities promoting the appropriate use of AI as a tool for NCUA employees to enhance productivity and noting that regulators who use AI technologies are more apt to understand why regulated entities use them.

In its November 2024 Artificial Intelligence Compliance Plan, the NCUA indicated it is taking a methodical approach to AI focusing on identifying AI tools of greatest utility to help the agency effectively and efficiently achieve its mission. NCUA must continue to assess controls and procedures such as the National Institute of Standards and Technology AI Risk Management Framework, which addresses maximizing positive impacts while minimizing negative impacts of AI.

Executive Order 13690, Promoting the Use of Trustworthy Artificial Intelligence in the Federal Government (December 2020), recognized the broad applicability of AI to be used by nearly every agency to improve operations, processes, and procedures, meet strategic goals, reduce costs, enhance oversight of the use of taxpayer funds, increase safety, train workforces, and support decision making. Agencies are encouraged to use AI appropriately to foster and maintain public trust and confidence.

My office's 2025 OIG Work Plan recognizes the need for NCUA to ensure AI accountability. The NCUA has focused on deploying AI solutions to automate or streamline various aspects of

the supervisory examination process and using AI for productivity, system monitoring, and data quality purposes. Recently, my office conducted investigations of employees who used public generative AI tools without authorization to conduct their work. Generative AI, which uses a model trained on large volumes of data and reinforced through feedback to refine the output, creates synthetic content that appears as if it is produced by a person. Generative AI can be viewed as transformative in its ability to innovate and streamline activities and disruptive due to privacy and security concerns, the potential for inaccuracy, or the potential to be used for crime or other illegal acts.

NCUA Bulletin 13600.2B, Employee Use of Artificial Intelligence (July 9, 2024) provided that NCUA employees and contractors may not use AI websites or tools that are not approved by the NCUA if their use involves submitting or exposing any non-public information, and may not install any unauthorized software, including AI, on NCUA owned or operated equipment or systems.

The use of AI to strengthen the agency, lead innovation, and generate efficiencies must be aligned with governance and risk management standards.