



NCUA
National Credit Union Administration

**OFFICE OF INSPECTOR
GENERAL**

**NATIONAL CREDIT UNION ADMINISTRATION
FEDERAL INFORMATION SECURITY MODERNIZATION
ACT OF 2014 AUDIT – FISCAL YEAR 2025**

**Report #OIG-25-08
August 20, 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*

SUBJECT: National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2025

DATE: August 20, 2025

Attached is the Office of Inspector General's FY 2025 independent evaluation of the effectiveness of the National Credit Union Administration's (NCUA) information security program and practices.¹

The OIG engaged Sikich CPA LLC (Sikich) to perform this evaluation.² The contract required that this evaluation be a performance audit performed in conformance with generally accepted government auditing standards issued by the Comptroller General of the United States.

The OIG monitored Sikich's performance under this contract, reviewed the report and its related documentation, and communicated with Sikich representatives. The OIG's monitoring and review was not intended to enable the OIG to express, and we do not express, an opinion on the matters contained in the report. Our monitoring and review found no instances in which Sikich did not comply with generally accepted government auditing standards.

This report summarizes the results of Sikich's independent performance audit and contains ten new recommendations that will assist the agency in improving the effectiveness of its information security and its privacy programs and practices. NCUA management concurred with and has identified corrective actions to address the recommendations.

We appreciate the effort, assistance, and cooperation NCUA management and staff provided to us and to Sikich management and staff during this engagement. If you have any questions on the report and its recommendations or would like to meet on this, please contact me at 703-518-6352.

¹ FISMA 2014, Public Law 113-283, requires Inspectors General to perform annual independent evaluations to determine the effectiveness of agency information security programs and practices.

² Sikich is an independent certified public accounting and consulting firm.

Distribution List:

Chairman Kyle S. Hauptman

Executive Director Larry Fazio

Chief of Staff Sarah Bang

General Counsel Frank Kressman

Acting Deputy Executive Director Towanda Brooks

Acting Deputy Executive Director Kelly Lay

Acting Chief Information Officer Amber Gravius

Chief Financial Officer Eugene Schied

Acting Chief Human Capital Officer Felicia Purifoy

Acting Deputy Chief Information Officer David Matheu

Acting Office of Examination and Insurance Director Amanda Parkhill

Office of External Affairs and Outreach Director Sierra Robinson

Office of Continuity and Security Management Director Kelly Gibbs

Senior Agency Office for Privacy Elizabeth Harris

Attachment

The background of the title section is a photograph of a classical building with large, fluted columns. An American flag is flying on a tall pole in the center. The image is overlaid with a semi-transparent light blue rectangle.

**PERFORMANCE AUDIT OF THE
NATIONAL CREDIT UNION ADMINISTRATION'S
IMPLEMENTATION OF THE
FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR
FISCAL YEAR 2025**

**SUBMITTED TO THE
OFFICE OF THE INSPECTOR GENERAL FOR THE
NATIONAL CREDIT UNION ADMINISTRATION**

PERFORMANCE AUDIT REPORT

AUGUST 20, 2025



333 John Carlyle Street, Suite 500
Alexandria, VA 22314
703.836.6701

SIKICH.COM

August 20, 2025

Marta Erceg
Acting Inspector General
National Credit Union Administration

Dear Acting Inspector General Erceg:

Sikich CPA LLC (Sikich) is pleased to submit the attached report detailing the results of our performance audit of the National Credit Union Administration's (NCUA's) information security program and practices for Fiscal Year (FY) 2025 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires federal agencies to perform an annual independent evaluation of their information security program and practices. FISMA states that the evaluation is to be performed by the agency's Inspector General (IG) or by an independent external auditor, as determined by the IG. The Office of the Inspector General for the NCUA engaged Sikich to conduct this performance audit.

The audit covered the period from October 1, 2024, through July 14, 2025. We performed the work from March through July 2025.

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective. We describe our objective, scope, and methodology in **Appendix B: Objective, Scope, and Methodology**.

We appreciate the assistance provided by NCUA management and staff.

Sincerely,

Sikich CPA LLC

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 1

II. AUDIT RESULTS..... 4

SECURITY FUNCTION: GOVERN..... 4

Finding 1: The NCUA Did Not Develop an Organizational Cybersecurity Profile or Related Policies and Procedures..... 5

SECURITY FUNCTION: IDENTIFY..... 7

Finding 2: The NCUA Did Not Maintain an Up-to-Date Inventory of Its Data and Corresponding Metadata..... 8

SECURITY FUNCTION: PROTECT..... 9

Finding 3: The NCUA Did Not Monitor Compliance with the Configuration Settings For All Networking Equipment..... 10

Finding 4: The NCUA Did Not Consistently Resolve Vulnerabilities for Workstations and a (b) (7)(E) Within the Required Timelines. 10

Finding 5: The NCUA Did Not Consistently Implement Account Management Controls..... 13

SECURITY FUNCTION: DETECT 16

SECURITY FUNCTION: RESPOND 17

SECURITY FUNCTION: RECOVER 17

APPENDIX A: BACKGROUND..... 19

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY 21

APPENDIX C: STATUS OF PRIOR-YEAR RECOMMENDATIONS..... 24

APPENDIX D: MANAGEMENT COMMENTS..... 28

I. EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. FISMA also requires agency Inspectors General (IGs) to assess the effectiveness of their agency's information security program and practices. The Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow. In addition, NIST issued the Federal Information Processing Standards (FIPS) to establish agency baseline security requirements.

The National Credit Union Administration (NCUA) Office of the Inspector General (OIG) engaged Sikich CPA LLC (Sikich) to conduct a performance audit in support of the FISMA requirement for an annual independent evaluation of the NCUA's information security program and practices. The objective of this performance audit was to assess the NCUA's compliance with FISMA and agency information security and privacy practices, policies, and procedures and ultimately to assess the effectiveness of the NCUA's information security program and practices.

The OMB and the Department of Homeland Security (DHS) annually provide federal agencies and IGs with instructions for preparing FISMA reports. On January 15, 2025, the OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.¹ This memorandum provides reporting guidance for Fiscal Year (FY) 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. The OMB, the Council of the Inspectors General on Integrity and Efficiency (CIGIE), and other stakeholders collaborated to develop the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0 (FY 2025 IG FISMA Reporting Metrics)*.²

The FY 2025 IG FISMA Reporting Metrics require us to assess the maturity of six function areas in the agency's information security program and practices. For this year's review, the FY 2025 IG FISMA Reporting Metrics required IGs to assess 20 core³ and 5 supplemental⁴ IG FISMA Reporting Metrics across 6 function areas—Govern,⁵ Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agency's information security program and the maturity level of each function area. The maturity levels are Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, Level 4: *Managed and Measurable*, and Level 5: *Optimized*. To be considered effective, an agency's information security program must be rated Level 4:

¹ See OMB Memorandum M-25-04 online [here](#).

² See the FY 2025 IG FISMA Reporting Metrics online [here](#).

³ Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine the effectiveness of a security program. The core metrics can be found in the FY 2025 IG FISMA Reporting Metrics online [here](#).

⁴ Supplemental metrics are assessed at least once every two years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of the effectiveness of the security program. The supplemental metrics can be found in the FY 2025 IG FISMA Reporting Metrics online [here](#).

⁵ In February 2024, NIST published the NIST Cybersecurity Framework (CSF) 2.0, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an entity's enterprise risk management strategy. As such, the FY 2025 IG FISMA Reporting Metrics added a new IG FISMA function (Govern) that includes a new domain (Cybersecurity Governance) to align with CSF 2.0.

Managed and Measurable or higher. See **Appendix A** for background information on the FISMA reporting requirements.

For this audit, we reviewed selected controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the FY 2025 IG FISMA reporting metrics, for a sample of 4 of the 62 NCUA-managed and third-party information systems⁶ in the NCUA's system inventory as of January 6, 2025. The audit covered the period from October 1, 2024, through July 14, 2025. We performed audit fieldwork from March through July 2025.

We concluded that the NCUA (1) implemented an effective information security program by achieving an overall maturity rating of Level 4: *Managed and Measurable*, (2) complied with FISMA, and (3) substantially complied with agency information security and privacy policies and procedures. **Table 1** below summarizes the NCUA's overall maturity levels for each Cybersecurity Framework (CSF) function and domain in the FY 2025 IG FISMA Reporting Metrics. We determined that two of the CSF function areas for the NCUA were at Maturity Level 5: *Optimized*, two were at Maturity Level 4: *Managed and Measurable*, and two were at Maturity Level 3: *Consistently Implemented*.

Table 1: Maturity Levels for FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions ⁷	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 4: <i>Managed and Measurable</i>	Cybersecurity Governance	Level 3: <i>Consistently Implemented</i> (Not Effective)
		Cybersecurity Supply Chain Risk Management (C-SCRM)	Level 5: <i>Optimized</i> (Effective)
Identify	Level 3: <i>Consistently Implemented</i>	Risk and Asset Management	Level 3: <i>Consistently Implemented</i>
Protect	Level 3: <i>Consistently Implemented</i>	Configuration Management	Level 2: <i>Defined</i> (Not Effective)
		Identity and Access Management	Level 4: <i>Managed and Measurable</i> (Effective)
		Data Protection and Privacy	Level 4: <i>Managed and Measurable</i> (Effective)
		Security Training	Level 4: <i>Managed and Measurable</i> (Effective)
Detect	Level 5: <i>Optimized</i>	Information Security and Continuous Monitoring (ISCM)	Level 5: <i>Optimized</i> (Effective)
Respond	Level 4: <i>Managed and Measurable</i>	Incident Response	Level 4: <i>Managed and Measurable</i> (Effective)
Recover	Level 5: <i>Optimized</i>	Contingency Planning	Level 5: <i>Optimized</i> (Effective)
Overall	Level 4: <i>Managed and Measurable</i> (Effective)		

Source: Sikich's assessment of the NCUA's information security program controls and practices based on the FY 2025 IG FISMA Reporting Metrics.

⁶ According to the [NIST Glossary](#), an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

⁷ See Appendix A, Tables 2 and 3, for definitions and explanations of the CSF functions and domains and maturity levels, respectively.

We determined that the NCUA established a number of information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, the NCUA:

- Continued to integrate cybersecurity risk management information into enterprise risk management (ERM) reporting tools.
- Implemented advanced ISCM technologies to analyze trends and identify potentially adverse events and adjusted its ISCM processes and security measures accordingly.
- Implemented supplier risk evaluations into its continuous monitoring practices to maintain situational awareness with regard to cyber-related supply chain risks.
- Implemented logging requirements at the Event Logging (EL) 1 maturity level (basic) and EL2 maturity level (intermediate), in accordance with OMB requirements.⁸
- Employed mechanisms to disrupt NCUA systems to test the effectiveness of its contingency planning processes.

Although we concluded that the NCUA's information security program was effective overall, its implementation of a subset of selected controls was not fully effective. Specifically, we identified five new weaknesses that fell in the Cybersecurity Governance, Configuration Management, Identity and Access Management, and Risk and Asset Management domains of the FY 2025 IG FISMA Reporting Metrics, as follows:

- The NCUA did not develop an organizational cybersecurity profile or related policies and procedures (**Finding 1: Govern Function – Cybersecurity Governance Domain**).
- The NCUA did not maintain an up-to-date inventory of its data and corresponding metadata (**Finding 2: Identify Function – Risk and Asset Management Domain**).
- The NCUA did not monitor compliance with the configuration settings for all networking equipment (**Finding 3: Protect Function – Configuration Management Domain**).
- The NCUA did not consistently resolve vulnerabilities for workstations and a (b) (7)(E) within the required timelines (**Finding 4: Protect Function – Configuration Management Domain**).
- The NCUA did not consistently implement account management controls (**Finding 5: Protect Function – Identity and Access Management Domain**).

⁸ OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, dated August 27, 2021, establishes a maturity model to guide the implementation of requirements across four EL tiers. OMB required agencies to meet the EL1 maturity level by August 28, 2022, and the EL2 maturity level by February 28, 2023.

In addition, the NCUA has outstanding prior-year recommendations that impact the IG FISMA Reporting Metrics. Specifically, at the beginning of FY 2025, the NCUA had 17 open recommendations from prior FISMA audits and evaluations for 2018,⁹ 2019,¹⁰ 2021,¹¹ 2022,¹² 2023,¹³ and 2024.¹⁴ During our FY 2025 audit, we determined that the NCUA took corrective actions to address 14 of these recommendations, and we consider those recommendations closed. Corrective actions are in progress for the other three open recommendations.¹⁵ In addition, the NCUA has one outstanding recommendation from a cybersecurity audit¹⁶ that impacts the incident response domain.

These prior-year control weaknesses, along with the new control weaknesses noted, affect the NCUA's ability to preserve the confidentiality, integrity, and availability of its information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction. As a result of the weaknesses noted in this audit, we made 10 new recommendations to assist the NCUA in strengthening its information security program and practices. Additionally, we noted that three prior-year recommendations remain open.¹⁷

The following section provides a detailed discussion of the audit results. **Appendix A** provides background information on FISMA. **Appendix B** describes the audit objective, scope, and methodology. **Appendix C** provides the status of prior-year FISMA report recommendations. **Appendix D** includes management's comments.

II. AUDIT RESULTS

The following section of the report describes the key controls underlying each function and domain and our assessment of the NCUA's implementation of those controls. We have organized our conclusions and ratings by function area and domain to help orient the reader to deficiencies as categorized by NIST CSF 2.0.

Security Function: Govern

The objective of the Govern function is to establish, communicate, and monitor an organization's cybersecurity risk management strategy, expectations, and policy. We determined that the maturity level of the NCUA's Govern function is Level 4: *Managed and Measurable*.

⁹ *FY 2018 Independent Evaluation of the National Credit Union Administration's Compliance with the Federal Information Security Modernization Act of 2014* (Report No. OIG-18-07, October 31, 2018).

¹⁰ *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit* (Report No. OIG-19-10, December 12, 2019).

¹¹ *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2021* (Report No. OIG-21-09, November 22, 2021).

¹² *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (Report No. OIG-22-07, October 26, 2022).

¹³ *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2023* (Report No. OIG-23-08, September 14, 2023).

¹⁴ *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024).

¹⁵ See Appendix C for the status of prior-year recommendations.

¹⁶ Recommendation 4, *National Credit Union Administration Cybersecurity Audit* (Report No. OIG-23-05, May 2, 2023).

¹⁷ See Appendix C for the status of prior-year recommendations.

Cybersecurity Governance

An agency with an effective cybersecurity governance program (1) monitors and reports on its progress in reaching target profiles and refines its organizational profiles periodically based on known risk exposure; (2) uses qualitative and quantitative data to assess the effectiveness of its cybersecurity risk management and integrates the cybersecurity risk management program into its ERM strategy; and (3) ensures that it has allocated adequate resources commensurate with cybersecurity responsibilities and uses qualitative and quantitative performance measures on the effectiveness of cybersecurity risk management roles.

We determined that the maturity level of the NCUA's Cybersecurity Governance domain is Level 3: *Consistently Implemented*. The NCUA continued to integrate cybersecurity risk management information into its ERM reporting tools and monitor its cybersecurity risk management program in near real time, leveraging predictive analytics and threat intelligence. However, the NCUA did not develop and maintain an organizational cybersecurity profile and document its policies, procedures, or guidance to facilitate developing and maintaining the profile (refer to **Finding 1** below).

Finding 1: The NCUA Did Not Develop an Organizational Cybersecurity Profile or Related Policies and Procedures.

The NCUA did not develop and maintain an organizational cybersecurity profile¹⁸ to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives in accordance with NIST CSF 2.0.¹⁹ In addition, the NCUA did not document its policies, procedures, or guidance for performing NIST CSF 2.0 activities to facilitate the development and maintenance of an organizational cybersecurity profile.

NCUA management stated that, although the NCUA's Information Security Program Policy directs the Office of the Chief Information Officer (OCIO) to develop and maintain an agency-wide information security program, including policies, procedures, and control techniques to address all applicable requirements for information security, the Information Security Program Policy does not specifically require the NCUA to develop and maintain current and target cybersecurity profiles.

Furthermore, NCUA management stated that the NCUA has aligned its cybersecurity program with the NIST CSF, providing artifacts to demonstrate how it governs and documents its current and target cybersecurity posture through various policies, procedures, controls, and risk management strategies.

However, our review determined that although these documents demonstrate the NCUA's implementation of its cybersecurity program, they fall short of the objective of the CSF organizational cybersecurity profile with regard to identifying the current status of the CSF functional outcomes and the target priority, to enable the NCUA to identify and analyze the differences between the current and target profiles.

¹⁸ NIST CSF 2.0 (February 26, 2024) provides guidance to assist with managing cybersecurity risks. Section 3.1 offers guidance on the use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives. A CSF organizational profile describes an organization's current and/or target cybersecurity posture in terms of the CSF core's outcomes. The CSF core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The CSF core components are a hierarchy of functions, categories, and subcategories that detail each outcome.

¹⁹ See the NIST CSF 2.0 online [here](#).

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), requires that:

Each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework)²⁰ developed by NIST, or any successor document, to manage the agency's cybersecurity risk.

Standards for Internal Control in the Federal Government (September 2014), GAO-14-704G, Principle 12 – Implement Control Activities, states that:

12.01 Management should implement control activities through policies.

Documenting current and target CSF profiles—including a gap analysis that identifies differences between the current and target state—decreases the risk that the agency may not have appropriately planned for or addressed cybersecurity risks. It may also reduce the risk of issues such as, but not limited to, breaches, system interruptions, and vulnerability exploitation.

To assist the NCUA in implementing the NIST CSF profiles, we recommend that NCUA management:

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.

Agency Response:

The NCUA concurs. The NCUA is actively addressing this recommendation through the development and refinement of cybersecurity governance documentation aligned with the NIST CSF 2.0. By March 31, 2026, the NCUA will update its cybersecurity program policy and procedures.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

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.

Agency Response:

The NCUA concurs. By March 31, 2027, the NCUA will document and maintain current and target cybersecurity profiles aligned with the NIST CSF 2.0.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

²⁰ Before version 2.0, the Cybersecurity Framework was called the *Framework for Improving Critical Infrastructure Cybersecurity*. This title is not used for NIST CSF 2.0.

Cybersecurity Supply Chain Risk Management

An agency with an effective C-SCRM program (1) reports qualitative and quantitative performance measures on the effectiveness of its supply chain risk management program, and (2) has incorporated supplier risk evaluations into its continuous monitoring practices.

We determined that the maturity level of the NCUA's C-SCRM domain is Level 5: *Optimized*. The NCUA has implemented processes for assessing and reviewing supply chain-related risks, such as 1) maintaining visibility into its upstream suppliers, 2) reporting qualitative and quantitative performance measures on the effectiveness of its C-SCRM program, and 3) analyzing, on a near real-time basis, the impact of changes to C-SCRM assurance²¹ requirements on its relationships with external providers.

In addition, we determined that NCUA completed corrective action to remediate a prior-year recommendation related to implementing a process to track and complete supply chain risk assessments for third-party systems and service providers.²²

We noted that the NCUA has an opportunity to enhance its C-SCRM program by completing implementation of one open prior-year recommendation related to documenting component authenticity procedures for preventing, detecting, and reporting counterfeit components.²³

Security Function: Identify

The objective of the Identify function is to ensure that the organization understands its cybersecurity risks. We determined that the maturity level of the NCUA's Identify function is Level 3: *Consistently Implemented*.

Risk and Asset Management

An agency with an effective risk and asset management program maintains an accurate inventory of information systems, hardware assets, and software assets; consistently implements its risk management policies, procedures, plans, and strategy at all levels of the organization; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its risk and asset management program.

We determined that the maturity level of the NCUA's Risk and Asset Management domain is Level 3: *Consistently Implemented*. The NCUA continued to integrate cybersecurity risk management information into its ERM reporting tools. In addition, the NCUA completed remediation of two prior FISMA recommendations related to completing annual system risk assessment reviews for third-party NCUA systems and services.²⁴

²¹ Assurance is confirmation that the software producer uses secure software development practices.

²² Recommendation 5, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024).

²³ Recommendation 1, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2021* (Report No. OIG-21-09, November 22, 2021).

²⁴ Recommendations 3 and 4, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024).

However, we noted that the NCUA has two open prior-year recommendations related to maintaining an up-to-date inventory of hardware assets.²⁵ In addition, we identified a new weakness in this domain related to the NCUA not maintaining an up-to-date inventory of its data and corresponding metadata.

Finding 2: The NCUA Did Not Maintain an Up-to-Date Inventory of Its Data and Corresponding Metadata.

The NCUA has not updated its inventory of data and the corresponding metadata for its data types since it initially developed the inventory in September 2021.

NCUA management stated that a full update of the comprehensive data inventory has been pending issuance of the OMB implementation guidance required by the 2018 Evidence Act.²⁶ The OMB issued this guidance in January 2025 (OMB Memorandum M-25-05), and it establishes a September 2026 deadline for action on the comprehensive data inventory. NCUA management further stated that the NCUA has kept the public data asset portion of its inventory up to date and available in the Federal Data Catalog at data.gov. The NCUA plans to take action to meet the requirements of OMB Memorandum M-25-05 by the established September 2026 deadline.

Public Law (Pub. L.) No. 115-435, *Foundations for Evidence-Based Policymaking Act of 2018*, Title II - Open Government Data Act, requires the head of each agency to, to the maximum extent practicable, develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency. The inventory is to provide a clear and comprehensive understanding of the data assets in the possession of the agency.

In addition, OMB issued guidance in Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*, which states:

4. Agency Requirements that Apply to All Data Assets
a. Comprehensive Data Inventories

Agencies must, to the maximum extent practicable, develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency (hereinafter "in the possession of the agency"), with the exception of data assets contained on a national security system. Data assets that are in the possession of, or shared by, more than one agency are required to be listed independently by each agency possessing those assets on the agency's comprehensive data inventory. Agencies must ensure that the comprehensive data inventory is clear and allows the public to understand all data assets in the possession of the agency.

²⁵ Recommendations 1 and 2, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024).

²⁶ The Evidence Act sets forth statutory requirements regarding federal evidence-building activities, open government data, and confidential information protection and statistical efficiency. Title II of the Evidence Act, also referred to as the Open, Public, Electronic, and Necessary (OPEN) Government Data Act ("OPEN Government Data Act" or "Act"), builds on long-running efforts to support the quality, accessibility, protection, and use of federal information and codifies many of the key aspects of the executive branch's 2013 open data policy. The OPEN Government Data Act established new requirements relating to data governance, management, and transparency.

Maintaining a comprehensive and accurate inventory of NCUA data and the corresponding metadata decreases the risk that the NCUA may not properly account for and secure sensitive data.

To assist the NCUA in maintaining its inventory of data and the corresponding metadata, we recommend that NCUA management:

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.

Agency Response:

The NCUA concurs. The NCUA completed an initial data inventory in 2021 while awaiting formal guidance from OMB. During this interim period, the agency prioritized the publication of up-to-date public data assets with full metadata in the Federal Data Catalog. However, to avoid duplicative efforts and inefficient use of staff and contractor resources, the NCUA paused updates to the data inventory and supporting systems until the full implementation requirements were released. With the January 2025 guidance now available, the NCUA established an integrated project team to complete update and meet the new requirements.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

Security Function: Protect

The objective of the Protect function is to ensure that organizations use safeguards to manage their cybersecurity risks. We determined that the maturity level of the NCUA's Protect function is Level 3: *Consistently Implemented*.

Configuration Management

An agency with an effective configuration management program employs automation to maintain an accurate view of the security configurations for all information system components connected to the agency's network; centrally manages its flaw remediation process; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its configuration management program.

We determined that the maturity level of the NCUA's Configuration Management domain is Level 2: *Defined*. Our review determined that the NCUA implemented standard baseline configurations for all platforms in its information technology (IT) environment except for routers, switches, and firewalls (refer to **Finding 3** below). In addition, our review determined that the NCUA made improvements in remediating vulnerabilities within the required timelines; however, we identified areas for continued improvement in the NCUA's vulnerability management program (refer to **Finding 4** below).

Finding 3: The NCUA Did Not Monitor Compliance with the Configuration Settings For All Networking Equipment.

Although the NCUA has defined secure configurations for its routers, switches, and firewalls, it does not currently perform compliance scans against these devices.

NCUA management stated that they do not perform compliance scans against these devices because the networking team is concerned the scans may disrupt network operations.

NCUA Information Security Manual, control CM-6, Configuration Settings, requires the NCUA to monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Monitoring networking devices against approved security configurations helps ensure that system configurations are secure, decreasing the risk of either intentional or inadvertent altering of configuration settings.

A prior FISMA recommendation addressed implementing, testing, and monitoring standard baseline configurations for all platforms in the NCUA information technology environment.²⁷ Because the NCUA has demonstrated improvements except for the areas noted above, we closed the prior recommendation and made one new targeted recommendation.

To assist the NCUA in implementing baseline compliance monitoring, we recommend that NCUA management:

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.

Agency Response:

The NCUA concurs. Baseline compliance monitoring for routers and switches has been implemented. The agency will extend this monitoring to include firewalls by no later than March 31, 2026. Any deviations from configuration baselines will be documented and supported with appropriate justifications.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

Finding 4: The NCUA Did Not Consistently Resolve Vulnerabilities for Workstations and (b) (7)(E) Within the Required Timelines.

The NCUA did not remediate 22 instances of critical- and high-risk vulnerabilities on workstations and one (b) (7)(E) within 30 and 60 days, respectively, as required by NCUA policy. Specifically, we noted the following:

²⁷ Recommendation 4, *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit* (Report No. OIG-19-10, December 12, 2019).

- Using the vulnerability scanning tool Nessus, which uses vulnerability data from the Common Vulnerability Scoring System (CVSS),²⁸ we identified unpatched software and improper configuration settings on workstations and a (b) (7)(E), as well as unsupported software on the (b) (7)(E), that exposed the NCUA network to critical²⁹ and high³⁰-severity vulnerabilities.
- Furthermore, the NCUA did not timely remediate six vulnerabilities that are on the Cybersecurity and Infrastructure Security Agency's (CISA's)³¹ Known Exploitable Vulnerabilities listing.³² Two of these vulnerabilities were on the workstations and four were on the (b) (7)(E).

NCUA management stated that the NCUA had not remediated the workstation vulnerabilities within the required timelines due to the workstations having been disconnected from the NCUA network for an extended period of time and then reconnected online. NCUA management has a process for following up on workstations for which the NCUA did not remediate vulnerabilities timely. However, we noted that the process did not effectively resolve workstation vulnerabilities.

In addition, NCUA management stated that the (b) (7)(E) personnel must physically come on site to patch each device. (The devices consist of Microsoft Windows workstations containing (b) (7)(E) software.) The (b) (7)(E) personnel only come on site once per month, and they therefore did not remediate some missing patches and improper configuration vulnerabilities within the defined patch timeframes. NCUA management further stated that the unsupported software occurred because (b) (7)(E) has not approved an upgrade for the (b) (7)(E). Furthermore, NCUA management stated that the (b) (7)(E) is in a segmented part of the network with restricted access. However, the vulnerabilities present still represent a risk if a malicious party gained access to the system.

NCUA Information Security Manual, Control SI-2, Flaw Remediation, specifies the following response times for remediating vulnerabilities:

For Non-Internet Accessible Systems and Laptops, the following NCUA-defined time periods for the release of the updates apply:

- *Critical Vulnerabilities (with CVSS score of 9 to 10) – 30 days*
- *High Vulnerabilities (with CVSS score of 7 to 8.9) – 60 days*

CISA Binding Operation Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, states that agencies are required to remediate each vulnerability in accordance with the timelines set forth in the CISA-managed vulnerability catalog. The catalog lists exploited vulnerabilities that carry significant risk to the federal enterprise and requires agencies to

²⁸ CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting the vulnerability's severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. CVSS is a published standard used by organizations worldwide.

²⁹ The critical rating is based on the CVSS, which provides a standardized way of reporting vulnerabilities based on the risk they pose to an organization. Critical vulnerabilities possess a rating of 10.

³⁰ High-risk vulnerabilities possess a CVSS rating of 7 to 9.9.

³¹ CISA, a component of DHS, is responsible for cybersecurity and infrastructure protection for all levels of government.

³² To help organizations better manage vulnerabilities and keep pace with threat activity, CISA maintains the authoritative source of vulnerabilities that have been exploited, along with the date by which agencies are required to remediate each vulnerability. See <https://www.cisa.gov/known-exploited-vulnerabilities-catalog> for more details.

remediate vulnerabilities within 6 months for vulnerabilities with a Common Vulnerabilities and Exposures (CVE)³³ ID assigned prior to 2021 and within 2 weeks for all other vulnerabilities. These default timelines may be adjusted in the case of grave risk to the federal enterprise.

By timely remediating vulnerabilities, the NCUA can mitigate its security weaknesses and limit the potential for attackers, including insider threats, to compromise the confidentiality, integrity, and availability of sensitive credit union and employee data, which will improve the overall security posture of the NCUA's information systems.

Prior FISMA recommendations addressed vulnerability remediation across the NCUA IT infrastructure.^{34 35 36} Because the NCUA has demonstrated improvement except for the areas noted above, we closed the prior recommendations and made three new targeted recommendations.

To assist the NCUA in ensuring consistent vulnerability management controls, we recommend that NCUA management:

Recommendation 5: Improve processes to ensure that the NCUA remediates workstation vulnerabilities within agency-required timelines, including monitoring for workstations that have been disconnected from the network for an extended period of time.

Agency Response:

The NCUA concurs. A small subset of workstations used for a specialized purpose by the Office of Continuity and Security Management were managed separately from all other workstations. The NCUA will explore solutions to ensure any such equipment is monitored and any vulnerabilities are remediated timely. This will be completed by September 30, 2026.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

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.

Agency Response:

The NCUA concurs and will implement a solution to address vulnerability remediation for this (b) (7)(E) including procedures for approving and documenting any deviations and compensating controls by September 30, 2026.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

³³ CVE is a list of all publicly known vulnerabilities that include the CVE ID.

³⁴ Recommendations 8 and 9, *FY 2018 Independent Evaluation of the National Credit Union Administration's Compliance with the Federal Information Security Modernization Act of 2014* (Report No. OIG-18-07, October 31, 2018).

³⁵ Recommendation 3, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (Report No. OIG-22-07, October 26, 2022).

³⁶ Recommendation 6, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024).

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

Agency Response:

The NCUA concurs and will address this as noted in the response to recommendation #6.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

Identity and Access Management

An agency with an effective identity and access management program ensures that all privileged and non-privileged users employ strong authentication for accessing organizational systems and uses automated mechanisms to assist in managing privileged accounts.

We determined that the maturity level of the NCUA's Identity and Access Management domain is Level 4: *Managed and Measurable*. The NCUA has demonstrated strengths in this area by enforcing multi-factor authentication for both privileged and non-privileged users for applicable NCUA systems. In addition, the NCUA has implemented an enterprise-wide single sign-on solution that its systems interface with.

Furthermore, the NCUA took corrective action to remediate prior-year recommendations related to implementing a solution that resolves a privileged access management vulnerability;³⁷ validating that server policies and/or related automated scripts are configured and running as desired when introducing a new server to the NCUA IT environment to identify inactive accounts;³⁸ and completing the 2024 backlog of overdue background reinvestigations.³⁹

However, we determined that the NCUA has opportunities to improve its identity and access management program by consistently implementing account management controls, as noted below.

Finding 5: The NCUA Did Not Consistently Implement Account Management Controls.

The NCUA did not perform the following account management processes in accordance with NCUA policy:

- Document approval for the total population of one new privileged⁴⁰ (b) (7)(E) (b) (7)(E) user account.

³⁷ Recommendation 4, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (Report No. OIG-22-07, October 26, 2022). See Appendix C for additional information regarding these prior-year recommendations.

³⁸ Recommendation 1, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2023* (Report No. OIG-23-08, September 14, 2023). See Appendix C for additional information regarding these prior-year recommendations.

³⁹ Recommendation 7, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024). See Appendix C for additional information regarding these prior-year recommendations.

⁴⁰ NIST defines a privileged user as a user that is authorized (and therefore trusted) to perform security-relevant functions that ordinary users are not authorized to perform.

- Complete the quarterly account reviews, including privileged user accounts for the (b) (7)(E) and (b) (7)(E) systems.
- Deactivate accounts after 30 days of inactivity for five privileged (b) (7)(E) users and one privileged (b) (7)(E) user.

Regarding the lack of approval for the (b) (7)(E) privileged user account, NCUA management stated that the NCUA has one (b) (7)(E) with two instances:⁴¹ (b) (7)(E) (b) (7)(E) in one instance and (b) (7)(E) in another instance. The (b) (7)(E) administrator for (b) (7)(E) is the same as the (b) (7)(E) administrator for (b) (7)(E), and the system owner believed that the (b) (7)(E) administrator account was approved for use in (b) (7)(E) because it was already approved for use in (b) (7)(E).

Regarding the lack of quarterly privileged user account reviews, NCUA management indicated that the system owner for (b) (7)(E) was unaware of a quarterly review requirement, given that (b) (7)(E) only has one active administrator account. NCUA management also stated that the NCUA has delegated account review responsibilities to the Information System Security Officer (ISSO), who is tasked with implementing and maintaining artifacts in accordance with the ISCM plan for their assigned systems and services. Although the NCUA assigned ISSOs to (b) (7)(E) and (b) (7)(E) the ISSOs did not communicate with the system owners regarding the ISCM requirements for NCUA system controls.

NCUA management further noted that the NCUA (b) (7)(E) ISSOs for 14 systems and 50 services, which impacts the ISSOs' ability to support system owners or designated system owners and ensure compliance with NCUA security policy. NCUA management indicated that, although the NCUA was in the process of hiring additional ISSO staff to support system owners, the current federal hiring freeze has prevented the NCUA from filling these positions.

NCUA management stated that, by design, the NCUA does not deactivate privileged (b) (7)(E) accounts when the users do not log in within 30 days of inactivity, as these accounts are necessary to maintain the platform and any related development activity. However, the NCUA did not document any risk-based decisions related to this issue, including identifying controls to compensate for not complying with agency policies.

In addition, NCUA management stated that the one privileged (b) (7)(E) user is a backup administrator who did not log in often but whose account was kept active in the event the other administrators were unable to perform their role. However, the NCUA did not document any risk-based decisions related to this issue, including identifying controls to compensate for not complying with agency policies. Upon our identification of this issue, NCUA management stated that they remediated the issue and that the account no longer remains active after 30 days of inactivity. We validated that the NCUA had remediated the issue.

NCUA *Information Security Manual*, Control AC-2, Account Management, requires the NCUA to 1) require approvals by appropriate personnel or roles for requests to create accounts, and 2) review accounts for compliance with account management requirements at least quarterly.

NCUA *Information Security Manual*, Control AC2(3), Account Management/Disable Accounts, requires the NCUA to disable accounts when they have been inactive for 30 days.

⁴¹ (b) (7)(E) uses a (b) (7)(E) such that each (b) (7)(E) customer receives their own instance or instances of the (b) (7)(E) Platform on which to run applications.

With effective account management controls, the NCUA can reduce the risk of unauthorized access to agency information, decreasing the likelihood of unauthorized modification, loss, and disclosure. In addition, by performing periodic account reviews, the NCUA can reduce the risk that system users whose job duties may have changed retain access that they no longer require. Lastly, by disabling inactive privileged user accounts in accordance with agency policy, the NCUA can reduce the risk that a bad actor may misuse these privileged accounts or that the accounts are susceptible to a brute-force attack to gain access to the NCUA's data or sensitive information or to perform significant actions, such as changing system configurations, installing software, and creating new user accounts.

To assist the NCUA in consistently implementing account management controls, we recommend that NCUA management:

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.

Agency Response:

The NCUA concurs. The issue has been remediated. A full review of all current (b) (7)(E) privileged user accounts has been completed.

OIG Response:

We concur with management's specified action and will validate remediation during the FY 2026 FISMA audit.

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

Agency Response:

The NCUA concurs. The agency completed the account review and will ensure the timely completion of these quarterly account reviews going forward.

OIG Response:

We concur with management's specified action and will validate remediation during the FY 2026 FISMA audit.

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.

Agency Response:

The NCUA concurs. By March 31, 2026, the agency will implement a process to automatically disable privileged (b) (7)(E) user accounts after 30 days of inactivity. Any specific use case deviations will be documented.

OIG Response:

We concur with management's specified action and will validate status during the FY 2026 FISMA audit.

Data Protection and Privacy

An agency with an effective data protection and privacy program maintains the confidentiality, integrity, and availability of its data; is able to assess its security and privacy controls, as well as its breach response capacities; and reports on qualitative and quantitative data protection and privacy performance measures.

We determined that the maturity level of the NCUA's Data Protection and Privacy domain is Level 4: *Managed and Measurable*. The NCUA has demonstrated strengths in this area by ensuring that its security controls for protecting personally identifiable information and other agency sensitive data are subject to monitoring processes. In addition, the NCUA integrates network defenses into its ISCM and incident response programs to provide near real-time monitoring of the data that is entering and exiting the network, as well as of other suspicious inbound and outbound communications. Furthermore, the NCUA completed remediation of a prior FISMA recommendation related to media marking for designating protection standards for safeguarding and/or disseminating agency information.⁴²

Security Training

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities through training or talent acquisition.

We determined that the maturity level for the NCUA's Security Training domain is Level 4: *Management and Measurable*. The NCUA has assessed the knowledge, skills, and abilities of its workforce, identified its skill gaps, and addressed the gaps through training. In addition, the NCUA completed the remediation of a prior FISMA recommendation related to strengthening its process for ensuring that it enrolls new hires in required role-based training.⁴³

Security Function: Detect

The objective of the Detect function is to ensure that organizations identify and analyze possible cybersecurity attacks and compromises. We determined that the maturity level of the NCUA's Detect function is Level 5: *Optimized*.

Information Security Continuous Monitoring

An agency with an effective ISCM program maintains ongoing authorizations of information systems; uses up-to-date cyber threat intelligence when analyzing logs; automates its inventory collection and anomaly detection to detect unauthorized devices; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its ISCM policies, procedures, plans, and strategies.

We determined that the maturity level for the NCUA's ISCM domain is Level 5: *Optimized*. The NCUA has fully integrated its ISCM policies and strategy with its enterprise and supply chain

⁴² Recommendation 6, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2021* (Report No. OIG-21-09, November 22, 2021). See Appendix C for additional information regarding these prior-year recommendations.

⁴³ Recommendation 8, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024). See Appendix C for additional information regarding these prior-year recommendations.

risk management, configuration management, incident response, and business continuity programs. In addition, the NCUA uses advanced ISCM technologies to analyze trends and identify potentially adverse events.

Security Function: Respond

The objective of the Respond function is to ensure that organizations take action regarding a detected cybersecurity incident. We determined that the maturity level of the NCUA's Respond function is Level 4: *Managed and Measurable*.

Incident Response

An agency with an effective incident response program:

- Uses profiling techniques to measure the characteristics of expected network and system activities so it can more effectively detect security incidents.
- Manages and measures the impact of successful incidents.
- Uses incident response metrics to measure and manage the timely reporting of incident information to organizational officials and external stakeholders.
- Consistently collects, monitors, and analyzes qualitative and quantitative performance measures on the effectiveness of its incident response policies, procedures, plans, and strategies.
- Meets EL maturity requirements.

We determined that the maturity level of the NCUA's Incident Response domain is Level 4: *Managed and Measurable*. The NCUA uses profiling techniques to measure the characteristics of expected activities on its networks and systems and has implemented logging requirements at the EL1 maturity level (basic) and EL2 maturity level (intermediate), in accordance with OMB requirements.⁴⁴

Security Function: Recover

The objective of the Recover function is to ensure that organizations restore assets and operations affected by a cybersecurity incident. We determined that the maturity level of the NCUA's Recover function is Level 5: *Optimized*.

Contingency Planning

An agency with an effective contingency planning program ensures that it integrates the results of business impact analyses (BIAs) with its ERM processes and uses these results to make senior-level decisions; employs automated mechanisms to thoroughly and effectively test system contingency plans; and communicates metrics on the effectiveness of recovery activities to relevant stakeholders.

⁴⁴ The NCUA has an open recommendation related to implementing requirements across the E1, EL2, and EL3 maturity levels to ensure that it logs and tracks events in accordance with OMB Memorandum M-21-31 (Recommendation 4, *National Credit Union Administration Cybersecurity Audit* [Report No. OIG-23-05, May 2, 2023]). Although our review showed that the NCUA has implemented EL1 and EL2 logging requirements, the open prior-year recommendations also require the NCUA to implement EL3 logging requirements.

We determined that the maturity level for the NCUA's Contingency Planning domain is Level 5: *Optimized*. The NCUA performed a full recovery and reconstitution of systems and proactively employed procedures to disrupt systems and system components to more effectively test the effectiveness of its contingency planning processes. In addition, the NCUA completed implementation of its new alternate processing and storage site and ensured that the site is in a fully operational state.⁴⁵

⁴⁵ Recommendation 9, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024). See Appendix C for additional information regarding these prior-year recommendations.

APPENDIX A: BACKGROUND

Federal Information Security Modernization Act of 2014

FISMA requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Agencies must also report annually to the OMB and to Congressional committees on the effectiveness of their information security program and practices. In addition, FISMA requires agency IGs to assess the effectiveness of their agency's information security program and practices.

NIST Security Standards and Guidelines

FISMA requires NIST to provide standards and guidelines pertaining to federal information systems. The standards prescribed include information security standards that provide the minimum information security requirements necessary to improve the security of federal information and information systems. FISMA also requires that federal agencies comply with NIST's FIPS. In addition, NIST develops and issues SPs as recommendations and guidance documents.

FISMA Reporting Requirements

The OMB and the DHS annually provide federal agencies and IGs with instructions for preparing FISMA reports. On January 15, 2025, the OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum provides reporting guidance for FY 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices. The OMB, the CIGIE, and other stakeholders collaborated to develop these metrics.

One of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving objectives that strengthen federal cybersecurity. The FY 2025 IG FISMA Reporting Metrics were updated to reflect recent developments:

- NIST published CSF 2.0 in February 2024, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's ERM strategy. The FY 2025 IG FISMA Reporting Metrics therefore added a new IG FISMA function (*Govern*) that includes a new domain (*Cybersecurity Governance*), to align with NIST CSF 2.0.
- To align with NIST CSF 2.0, the C-SCRM domain moved from the *Identify* function to the *Govern* function, to better reflect agency oversight of supply chain risk.
- The FY 2025 IG FISMA Reporting Metrics introduced a new domain, Risk and Asset Management, in the *Identify* function to group metrics on system inventory and hardware, software, and data management.
- Five supplemental metrics are in scope for the FY 2025 IG FISMA evaluation, including two new supplemental metrics that are focused on system-level risk management practices critical to achieving Zero Trust Architecture objectives.

- The FY 2025 IG FISMA Reporting Metrics revised the core metric on information system-level risk management to focus on the maturity of agencies' implementation of the NIST Risk Management Framework.

As highlighted in **Table 2**, the FY 2025 IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and practices and align with the six function areas in NIST CSF 2.0: Govern, Identify, Protect, Detect, Respond, and Recover.

Table 2: Alignment of the CSF Functions to the Domains in the FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance and C-SCRM
Identify	The organization's current cybersecurity risks are understood.	Risk and Asset Management
Protect	Safeguards to manage the organization's cybersecurity risks are used.	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	ISCM
Respond	Actions regarding a detected cybersecurity incident are taken.	Incident Response
Recover	Assets and operations affected by a cybersecurity incident are restored.	Contingency Planning

Source: Sikich's analysis of NIST CSF 2.0 and the FY 2025 IG FISMA Reporting Metrics

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 3** below explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of at least Level 4: *Managed and Measurable*.

Table 3: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess the policies and procedures and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2025 IG FISMA Reporting Metrics

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this performance audit was to assess the NCUA’s compliance with FISMA and agency information security and privacy practices, policies, and procedures and ultimately to assess the effectiveness of the NCUA’s information security program and practices.

Scope

The scope of this performance audit covered the NCUA’s information security program and practices consistent with FISMA and reporting instructions that the OMB and the DHS issued for FY 2025. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, to support the FY 2025 IG FISMA Reporting Metrics for a sample of 4 of 62 NCUA-managed information systems and third-party information systems in the NCUA’s system inventory as of January 6, 2025 (**Table 4**).

Table 4: Description of System Selected for Testing

System Name	Description
NCUA General Support System (GSS) (NCUA-managed system)	The NCUA GSS provides the computing platform for all significant business applications of the NCUA. The platform includes all major IT hardware, software, communications, network storage, central databases, operating systems, and other minor, infrastructure, security-related, and productivity applications.
Enterprise Central Data Repository (ECDR) (NCUA-managed system)	ECDR is an enterprise data repository and Business Intelligence (BI) solution that provides the central location for storing and managing NCUA’s enterprise data for analytics and reporting. ECDR applies an end-to-end BI platform that supports: a) data discovery and information integration; b) metadata management; c) enterprise data sharing via a Web application programming interface; and d) analytics and reporting capabilities. The system also provides authorized privileged users access to specific dashboards and reports, in addition to system administrative accounts.
FOIAXpress (third-party system)	FOIAXpress is a Federal Risk and Authorization Management Program (FedRAMP) authorized ⁴⁶ cloud-based software-as-a-service case management suite. NCUA’s Office of General Counsel uses FOIAXpress to fulfill its responsibility for processing Freedom of Information Act requests and appeals, as well as Privacy Act requests.
Cyber Incidents for Credit Unions Reporting System (CICURS) (third-party system)	CICURS is a system built on a ServiceNow platform designed to receive and track reportable cyber incidents from federally insured credit unions, analyze incidents for cyber threats and vulnerabilities, and develop response measures.

Source: NCUA System Inventory

For this year’s review, IGs were required to assess 20 core and 5 supplemental IG FISMA Reporting Metrics across six function areas—Govern, Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of their agency’s information security program and the maturity level of each function area.

⁴⁶ FedRAMP is a governmentwide program that provides a standardized approach to security assessment, authorization, and continuous monitoring for cloud products and services. [FedRAMP | GSA](#)

The audit also included an evaluation of whether the NCUA took corrective actions to address open recommendations from the FY 2018 FISMA evaluation,⁴⁷ and the FY 2019,⁴⁸ FY 2021,⁴⁹ FY 2022,⁵⁰ FY 2023,⁵¹ and FY 2024 FISMA audits.⁵²

The audit covered the period from October 1, 2024, through July 14, 2025. We performed audit fieldwork from March through July 2024.

Methodology

We conducted this performance audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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 objective. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our audit objective, we completed the following procedures:

- Evaluated key components of the NCUA's information security program and practices, consistent with FISMA and with reporting instructions that the OMB and the DHS issued for FY 2025.
- Focused our testing activities on assessing the maturity of the 20 core and 5 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Performed inquiries of NCUA management and staff.
- Considered guidance contained in OMB's Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, when planning and conducting our work.
- Evaluated select security processes and controls at the program level, as well as for a non-statistical sample of 4 NCUA-managed and third-party information systems from the 62 systems in the NCUA's system inventory. We considered the NCUA's reliance on third-party systems and the purpose of each of the NCUA's information systems and selected 2 of the 13 NCUA-managed systems and 2 of the 49 third-party systems for testing this year. All four systems selected for testing are designated as moderate-impact systems based on NIST FIPS 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- Analyzed the sample of four systems selected for testing, including reviewing selected system documentation and other relevant information, as well as testing selected security controls to support the IG FISMA Reporting Metrics.
- Reviewed the status of prior-year FISMA recommendations. See **Appendix C** for the status of the prior-year recommendations.

⁴⁷ See Footnote 9.

⁴⁸ See Footnote 10.

⁴⁹ See Footnote 11.

⁵⁰ See Footnote 12.

⁵¹ See Footnote 13.

⁵² See Footnote 14.

The *FY 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2025 FISMA audit. As part of this approach, IGs must average the ratings for core and supplemental IG FISMA Reporting Metrics independently to determine a domain's maturity level and provide data points for the assessed effectiveness of the program and function. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, the IG FISMA Reporting Metrics do not automatically round calculated averages to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, the OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie directly to administration priorities and other high-risk areas. The OMB recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the FY 2025 IG FISMA Reporting Metrics guidance⁵³ to form our conclusions for each CSF domain and function, as well as for the overall agency rating. Specifically, we focused on the calculated average scores of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting Metrics and progress that the NCUA has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

Our work did not include assessing the sufficiency of internal controls over the NCUA's information security program or other matters not specifically outlined in this report.

⁵³ The FY 2025 IG FISMA Reporting Metrics provided the agency IG with the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency information security program is effective at a calculated maturity level lower than level 4.

APPENDIX C: STATUS OF PRIOR-YEAR RECOMMENDATIONS

The table below summarizes the status of the open prior-year recommendations from the FY 2018 FISMA evaluation and the FY 2019, FY 2021, FY 2022, FY 2023, and FY 2024 FISMA audits.⁵⁴ At the time of testing and IG FISMA Reporting Metric submission, 3 of the 17 prior-year recommendations from the audits referenced above remained open.

In the following table, the “Auditor’s Position on Status” column is based on our inspection of evidence received during fieldwork. The auditors will follow up on the open prior-year recommendations recorded in this report during the next audit cycle. Additionally, this table maps the prior-year recommendation to the affected IG FISMA Reporting Metric domains.

Report No. Recommendation No.	Recommendation	Auditor’s Position on Status	Affected IG FISMA Reporting Metric Domains
OIG-24-08 Recommendation 1	We recommend that NCUA management conduct refresher training for the PCs regarding documenting and maintaining asset management system records in accordance with NCUA policy and procedures.	Open We inquired with NCUA personnel and determined that the NCUA has not completed remediation of this recommendation. The NCUA provided an estimated completion date of September 30, 2025.	Risk and Asset Management
OIG-24-08 Recommendation 2	We recommend that NCUA management update the accountable property policy to implement a process for the PMO 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.	Open We inquired with NCUA personnel and determined that the NCUA has not completed remediation of this recommendation. The NCUA provided an estimated completion date of September 30, 2025.	Risk and Asset Management
OIG-24-08 Recommendation 3	We recommend that NCUA management complete the PRISM risk assessment review on an annual basis and document the results.	Closed We inspected evidence that the NCUA had completed the PRISM risk assessment review on an annual basis and documented the results.	Risk and Asset Management
OIG-24-08 Recommendation 4	We recommend that NCUA management ensure that the annual risk assessment reviews for all third-party NCUA services are completed.	Closed We inspected evidence that the NCUA had completed risk assessment reviews for all third-party NCUA services.	Risk and Asset Management
OIG-24-08 Recommendation 5	We recommend that NCUA management document and implement a process to track and complete	Closed	C-SCRM

⁵⁴ See Footnotes 9, 10, 11, 12, 13, and 14.

Report No. Recommendation No.	Recommendation	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	supply chain risk assessments for all third-party systems and service providers.	We inspected evidence that the NCUA had tracked and completed supply chain risk assessments for all third-party systems and service providers.	
OIG-24-08 Recommendation 6	We recommend that NCUA management implement improved processes for leveraging dashboards in order to monitor and manage patch compliance and remediation of vulnerabilities including the tracking of approved and unapproved software.	Closed We inspected evidence that the NCUA had implemented dashboards for monitoring and managing patch compliance and remediation of vulnerabilities, including tracking approved and unapproved software.	Configuration Management
OIG-24-08 Recommendation 7	We recommend that NCUA management complete the 2024 backlog of overdue reinvestigations.	Closed We inspected evidence that the NCUA had completed the 2024 backlog of overdue reinvestigations.	Identity and Access Management
OIG-24-08 Recommendation 8	We recommend that NCUA management document and implement a process for notifying Office of Human Resources to add the initial role-based security training requirement to the learning profile in the learning management system for new hires requiring the training.	Closed We inspected evidence that the NCUA had documented and implemented a process for notifying the OHR to add the initial role-based security training requirement to the learning profile in the learning management system for new hires requiring the training.	Security Training
OIG-24-08 Recommendation 9	We recommend that NCUA management complete implementation of the new alternate processing and storage site to a fully operational state.	Closed We inspected evidence that the NCUA had completed implementation of the new alternate processing and storage site and ensured that the site was in a fully operational state.	Contingency Planning
OIG-23-08 Recommendation 1	We recommend that NCUA management document and implement a process to validate that server policies and/or related automated scripts are configured and running as desired when introducing a new server to the NCUA information technology environment.	Closed We inspected evidence that the NCUA had documented a process to validate that server policies and/or related automated scripts are configured and running as desired when introducing a new server to the NCUA IT environment. The NCUA did not introduce any new servers to the environment this fiscal year; however, because the NCUA has documented a process to remediate the control weakness, we closed the recommendation.	Identity and Access Management

Report No. Recommendation No.	Recommendation	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
OIG-22-07 Recommendation 3	We recommend that NCUA conduct an analysis of the technologies employed within the NCUA operational environment and document a plan to reduce the wide variety of differing technologies requiring support and vulnerability remediation, as feasible.	Closed We inspected evidence that the NCUA had conducted an analysis of the technologies employed within the NCUA operational environment and documented a plan to reduce the wide variety of differing technologies requiring support and vulnerability remediation.	Configuration Management
OIG-22-07 Recommendation 4	We recommend that NCUA implement a solution that resolves the privileged access management vulnerability.	Closed We inspected evidence that the NCUA had implemented a solution that resolves the privileged access management vulnerability.	Identity and Access Management
OIG-21-09 Recommendation 1	We recommend that NCUA review the SCRM NIST guidance and update the SCRM plan, policies, and procedures to fully address supply chain risk management controls and practices.	Open We noted that the NCUA has not defined and communicated its component authenticity policies and procedures in accordance with NIST requirements. The NCUA provided an estimated completion date of September 30, 2025.	C-SCRM
OIG-21-09 Recommendation 6	We recommend that NCUA upon issuance of the CUI policies, design and implement media marking to designate protection standards for safeguarding and/or disseminating agency information.	Closed We inspected evidence that the NCUA had designed and implemented media marking to designate protection standards for safeguarding and/or disseminating agency information.	Data Protection and Privacy
OIG-19-10 Recommendation 4	We recommend that NCUA ensures the Agency implements, tests, and monitors standard baseline configurations for all platforms in the NCUA information technology environment in compliance with established NCUA security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Closed We noted that the NCUA had implemented standard baseline configurations for all platforms except for routers, switches, and firewalls. We therefore closed this recommendation and made a new targeted recommendation. See Finding 3.	Configuration Management
OIG-18-07 Recommendation 8	We recommend that the Office of Chief Information Officer enforce the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.	Closed We noted that the NCUA had demonstrated improvements in remediating patch and configuration-related vulnerabilities within agency-defined timeframes across the NCUA IT infrastructure, except for workstations and a third-party system. We therefore closed this	Configuration Management

Report No. Recommendation No.	Recommendation	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
		recommendation and made new targeted recommendations. See Finding 4.	
OIG-18-07 Recommendation 9	We recommend that the Office of the Chief Information Officer implement a process to detect and migrate unsupported software to supported platforms before support for the software ends.	Closed We noted that the NCUA had demonstrated improvements in implementing a process to detect and migrate unsupported software to supported platforms across the NCUA IT infrastructure, except for a third-party system. We therefore closed this recommendation and made a new targeted recommendation. See Finding 4.	Configuration Management

APPENDIX D: MANAGEMENT COMMENTS



NATIONAL CREDIT UNION ADMINISTRATION
Office of the Executive Director

SENT BY EMAIL

TO: Acting Inspector General Marta Erceg

FROM: Executive Director Larry Fazio

LARRY
FAZIO

Digitally signed by
LARRY FAZIO
Date: 2025.08.06
17:03:43 -0400

SUBJ: FISMA Act of 2014 Fiscal Year 2025 Audit Draft Report

DATE: August 6, 2025

Thank you for the opportunity to review and comment on the draft report for the *Federal Information Security Modernization Act of 2014 (FISMA) Audit for Fiscal Year (FY) 2025*. The draft report concludes that the NCUA has implemented an effective information security program, achieved an overall Level 4 – *Managed and Measurable* maturity level, and complied with FISMA. The NCUA's overall maturity level reflects its continuing commitment to strong information security.

The draft report makes ten new recommendations to assist the NCUA in further strengthening its information security program. Responses to the draft report's recommendations and other aspects of the report are provided below.

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.

Management Response: The NCUA concurs. The NCUA is actively addressing this recommendation through the development and refinement of cybersecurity governance documentation aligned with the National Institute of Standards and Technology (NIST) Cybersecurity Framework (CSF) 2.0. By March 31, 2026, the NCUA will update its cybersecurity program policy and procedures.

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.

Management Response: The NCUA concurs. By March 31, 2027, the NCUA will document and maintain current and target cybersecurity profiles aligned with the NIST CSF 2.0.

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 the Office of Management and Budget (OMB) Memorandum M-25-05 by the established September 2026 deadline.

Management Response: The NCUA concurs.

The NCUA completed an initial data inventory in 2021 while awaiting formal guidance from OMB. During this interim period, the agency prioritized the publication of up-to-date public data assets with full metadata in the Federal Data Catalog. However, to avoid duplicative efforts and inefficient use of staff and contractor resources, the NCUA paused updates to the data inventory and supporting systems until the full implementation requirements were released. With the January 2025 guidance now available, the NCUA established an integrated project team to complete update and meet the new requirements.

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.

Management Response: The NCUA concurs. Baseline compliance monitoring for routers and switches has been implemented. The agency will extend this monitoring to include firewalls by no later than March 31, 2026. Any deviations from configuration baselines will be documented and supported with appropriate justifications.

Recommendation #5

Improve processes to ensure that the NCUA remediates workstation vulnerabilities within agency-required timelines, including monitoring for workstations that have been disconnected from the network for an extended period of time.

Management Response: The NCUA concurs. A small subset of workstations used for a specialized purpose by the Office of Continuity and Security Management were managed separately from all other workstations. The NCUA will explore solutions to ensure any such equipment is monitored and any vulnerabilities are remediated timely. This will be completed by September 30, 2026.

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.

Management Response: The NCUA concurs and will implement a solution to address vulnerability remediation for this (b) (7)(E) including procedures for approving and documenting any deviations and compensating controls by September 30, 2026.

Recommendation #7

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

Management Response: The NCUA concurs and will address this as noted in the response to recommendation #6.

Page 3

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.

Management Response: The NCUA concurs. This issue has been remediated. A full review of all current (b) (7)(E) privileged user accounts has been completed.

Recommendation #9

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

Management Response: The NCUA concurs. The agency completed the account review and will ensure the timely completion of these quarterly account reviews going forward.

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.

Management Response: The NCUA concurs. By March 31, 2026, the agency will implement a process to automatically disable privileged (b) (7)(E) user accounts after 30 days of inactivity. Any specific use case deviations will be documented.

Please contact Acting Deputy Executive Director Towanda Brooks if you have any questions.

cc: Chief of Staff Bang
OEAC Director Robinson
DED Brooks