NCUA
National Credit Union Administration

Office of Inspector General

OIG-26-09

National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2026

August 13, 2026

NCUA

OFFICE OF INSPECTOR GENERAL

Memorandum

SENT BY EMAIL

DATE: August 13, 2026

TO: See Distribution List

FROM: Acting Inspector General Marta Erceg
Office of Inspector General

SUBJECT: National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2026

Attached is the Office of Inspector General's FY 2026 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 five 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

[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.

on the report and its recommendations or would like to meet on this, please contact me at 703-518-6352.

Distribution List:

NCUA Board (vacant)
Executive Director Larry Fazio
Acting Chief of Staff Nathan Kreoger
Acting Deputy Executive Director Kelly Lay
General Counsel Frank Kressman
Office of External Affairs and Outreach Director Sierra Robinson
Acting Chief Information Officer Amber Gravius
Acting Deputy Chief Information Officer David Matheu
Acting Examination & Insurance Director Amanda Parkhill
Acting Chief Financial Officer Melissa Lowden
Office of Human Resources Director Joe Hannah
Senior Agency Official for Privacy Elizabeth Harris

Attachment

SIKICH®

National Credit Union Administration

Implementation of the
Federal Information Security Modernization Act of 2014 for
Fiscal Year 2026
Performance Audit Report

AUGUST 11, 2026

sikich.com

333 John Carlyle Street, Suite 500
Alexandria, VA 22314
+1 (703) 836-6701

sikich.com

August 11, 2026

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) 2026 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, 2025, through July 13, 2026. We performed audit fieldwork from March through July 2026.

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

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 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) provide federal agencies and IGs with instructions for preparing annual 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] which provides reporting guidance for 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 *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (IG FISMA Reporting Metrics).[2]

The IG FISMA Reporting Metrics require us to assess the maturity of six Cybersecurity Framework (CSF)[3] function areas in the agency's information security program and practices. For this year's review, IGs were required to assess 20 core[4] and 5 supplemental[5] IG FISMA Reporting Metrics across 6 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. The maturity levels are Level 1: *Ad Hoc*, Level 2: *Defined*, Level 3: *Consistently Implemented*, Level 4: *Managed and Measurable*, and Level 5: *Optimized*.

[1] For FY 2026, OMB and DHS did not issue the annual FISMA instructions; we therefore performed the audit using the OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*. See OMB Memorandum M-25-04 online here.
[2] On March 17, 2026, the OMB and CIGIE, issued a joint communication directing IGs and independent external auditors to use the FY 2025 IG FISMA Reporting Metrics for FY 2026 FISMA audits. See the FY 2025 IG FISMA Reporting Metrics online here.
[3] The IG FISMA Reporting Metrics align with the six functions in the NIST Cybersecurity Framework 2.0 (CSF): *Govern, Identify, Protect, Detect, Respond, and Recover.* The CSF provides agencies with a common structure for managing and reducing their cybersecurity risks across the enterprise and provides IGs with guidance for assessing the maturity of controls to address those risks.
[4] 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.
[5] Supplemental metrics are metrics that are not considered core but 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.

To be considered effective, an agency's information security program must be rated Level 4: *Managed and Measurable* or higher. See **Appendix A** for background information on the FISMA reporting requirements.

For this audit, we reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the IG FISMA Reporting Metrics, for a sample of 4 of the 67 NCUA-managed and third-party information systems[6] in the NCUA's system inventory as of January 29, 2026. The audit covered the period from October 1, 2025, through July 13, 2026. We performed audit fieldwork from March through July 2026.

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 CSF function and domain in the IG FISMA Reporting Metrics. We determined that one of the CSF function areas for the NCUA was at Maturity Level 5: *Optimized*, three were at Maturity Level 4: *Managed and Measurable*, and two were at Maturity Level 3: *Consistently Implemented*.

Table 1: Maturity Levels for IG FISMA Reporting Metrics

CSF Functions[7]	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 4: *Managed and Measurable*	Cybersecurity Governance	Level 4: *Managed and Measurable*
		Cybersecurity Supply Chain Risk Management (C-SCRM)	Level 5: *Optimized*
Identify	Level 3: *Consistently Implemented*	Risk and Asset Management	Level 3: *Consistently Implemented*
Protect	Level 3: *Consistently Implemented*	Configuration Management	Level 2: *Defined*
		Identity and Access Management	Level 5: *Optimized*
		Data Protection and Privacy	Level 4: *Managed and Measurable*
		Security Training	Level 2: *Defined*
Detect	Level 4: *Managed and Measurable*	Information Security and Continuous Monitoring (ISCM)	Level 4: *Managed and Measurable*
Respond	Level 4: *Managed and Measurable*	Incident Response	Level 4: *Managed and Measurable*
Recover	Level 5: *Optimized*	Contingency Planning	Level 5: *Optimized*
Overall	**Level 4: *Managed and Measurable* (Effective)**		

Source: Sikich's assessment of the NCUA's information security program controls and practices based on the 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 the definitions and explanations of the CSF functions and domains and the IG FISMA Reporting Metrics 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:

- Developed a current and target cybersecurity profile and is implementing an action plan to address gaps between its current and target profile.
- Developed an inventory of its data and corresponding metadata for its data types and assigned data classifications to the data types.
- Consistently implemented processes for provisioning, managing, and reviewing privileged accounts in accordance with the NCUA's policies and procedures.
- Implemented advanced event logging requirements.

In addition, the NCUA took corrective actions to address all 13 prior-year recommendations from prior FISMA audits for 2021,[8] 2024[9] and 2025[10] and we consider those recommendations closed.

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 three weaknesses that fell in the Risk and Asset Management, Configuration Management, and Security Training domains of the IG FISMA Reporting Metrics, as follows:

- The NCUA did not fully document an accurate and complete record of hardware assets (**Finding 1**: Identify Function – Risk and Asset Management Domain).
- The NCUA did not fully implement baseline configurations in compliance with its established standard configurations (**Finding 2**: Protect Function – Configuration Management Domain).
- The NCUA did not periodically update its workforce assessment of the skills, knowledge, and abilities of its cybersecurity professionals to account for a changing risk environment (**Finding 3**: Protect Function – Security Training Domain).

These control weaknesses 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 five new recommendations to assist the NCUA in strengthening its information security program and practices.

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.

[8] *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2021* (Report No. OIG-21-09, November 22, 2021).
[9] *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2024* (Report No. OIG-24-08, September 12, 2024).
[10] *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2025* (Report No. OIG-25-08, August 20, 2025).

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*.

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 Enterprise Risk Management (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 4: *Managed and Measurable*. The NCUA developed a current and target cybersecurity profile and is implementing an action plan to address gaps between its current and target profile. In addition, 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.

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 assurance[11] requirements on its relationships with external providers.

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*.

[11] Assurance is confirmation that the software producer uses secure software development practices.

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 ensures that the information systems included in its inventory are subject to monitoring processes. In addition, the NCUA consistently implements an automated solution across the enterprise that provides a centralized, enterprise-wide view of cybersecurity risks.

However, although the NCUA took corrective action to address prior-year recommendations related to hardware asset[12] inventory training and monitoring,[13] hardware asset inventory issues remained, as discussed in **Finding 1** below.

Finding 1: The NCUA did not fully document an accurate and complete record of hardware assets.

The NCUA did not fully document an accurate and complete record of hardware assets. Specifically based on our review of the hardware asset inventory, we noted the following:

- 16 "In Use" hardware assets were not recorded as assigned to an individual or a location.
- For 418 "In Use" hardware assets that were not assigned to an individual, the location listed was not at a level of granularity necessary for tracking and reporting. Specifically, the locations only indicated Central Office, Asset Management & Assistance Center, Regional Sites, and Virginia and did not include more precise details such as specific rooms.

NCUA management stated that the Property Custodian (PC) did not ensure complete data entry for the individual the asset was assigned to, or the location of the asset. The NCUA has since conducted PC training that included information regarding the required fields for property records on April 28, 2026. In addition, the Property Management Officer (PMO) did not have sufficient time to complete a periodic review of the asset management system data since the *Accountable Property Operations Handbook (APOH)* was updated with that requirement in December 2025.

NCUA management also stated that the variances in specified asset assignment and location occurred because the existing inventory process does not fully capture the level of detail needed. While the NCUA tracks all deployed hardware assets, the procedures in place do not require documenting more granular location information (e.g., specific rooms or workspaces) for certain asset types. As a result, some items were recorded with general organizational locations instead of more specific identifiers.

[12] NIST defines a hardware asset as a physical component of an organization's technology infrastructure that has value to stakeholders. Examples of hardware assets included in the NCUA inventory included laptops, printers, smart phones, routers and switches.
[13] 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).

The NCUA *Configuration Management Control Family Document*, version 2.0, dated February 9, 2026, control CM-8, System Component Inventory, requires developing and documenting an inventory of system components that is at the level of granularity deemed necessary for tracking and reporting.

The NCUA Instruction NO. 1710.6, *Receipt, Transfer, and Disposal of Accountable Property*, dated September 27, 2019, requires the PMO to ensure that all accountable property is tracked, accounted for, and correctly reported as necessary.

The NCUA APOH, dated December 2025, section 5.1 Record Creation requires the PC to create an asset management system record for accountable property that includes among other things the location of the asset and/or the person the asset is assigned to. In addition, section 2.1 PMO requires the PMO to complete periodic reviews of the asset management system data to validate that the inventory is documented and maintained in accordance with NCUA Instruction 1710.6 and the APOH.

An accurate and complete hardware asset inventory ensures that every asset has a documented responsible individual or precise location. If hardware asset locations are properly tracked, the risk of devices being stolen, moved, misplaced, or accessed without detection can be decreased. In addition, the NCUA would decrease its risk of data loss, including the loss of personally identifiable information.

To assist the NCUA with ensuring that it documents and maintains a complete and accurate hardware asset inventory at the level of granularity necessary for tracking and reporting, we recommend that NCUA management:

Recommendation 1: Update the NCUA *Accountable Property Operations Handbook* to require documenting more granular location information (e.g., specific rooms or workspaces) for applicable asset types.

Agency Response:
NCUA agrees and will implement this recommendation by March 31, 2027.

OIG Response:
We acknowledge NCUA's concurrence with this recommendation.

Recommendation 2: Validate that the Property Management Officer completes periodic reviews of the asset management system data to confirm the inventory is documented and maintained in accordance with NCUA Instruction 1710.6 and the *Accountable Property Operations Handbook*.

Agency Response:
NCUA agrees and will implement this recommendation by March 31, 2027.

OIG Response:
We acknowledge NCUA's concurrence with the recommendation.

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.* The NCUA implemented flaw remediation policies, procedures, and processes for remediating vulnerabilities in accordance with the NCUA's established timelines. In addition, the NCUA took corrective action to close a prior-year recommendation related to baseline compliance monitoring for routers, switches, and firewalls on the NCUA network.[14] However, our review also determined that the NCUA did not fully implement baseline configurations in compliance with its established standard configurations, as discussed in **Finding 2** below.

Finding 2: The NCUA did not fully implement baseline configurations in compliance with its established standard configurations.

The NCUA did not fully implement baseline configurations in compliance with its established standard configurations. Specifically, we noted:

- Of the (b) (7)(E) Windows 11 devices, compliance ranged from 31 to 76 percent.
- Of the (b) (7)(Windows Server (b) (7)(E) devices, (b) (7)(ranged from 48 to 89 percent compliant; the remaining (b) (7)(E devices were above 90 percent compliant, but none were at 100 percent compliance.
- Of the (b) (7)(E Windows Server (b) (7)(E) devices, (b) (7)(ranged from 60 to 89 percent compliant; the remaining (b) (7)(devices were above 90 percent compliant, but none were at 100 percent compliance.
- The (b) (7)(Windows Server (b) (7)(E) devices ranged from 93 to 98 percent compliant.
- The (b) (7)((b) (7)(E) devices ranged from 84 to 95 percent compliant.
- The (b) (b) (7)(E) firewall devices ranged from 84 to 97 percent compliant.

NCUA management stated that it has established baseline configurations and has documented approved deviations through its risk acceptance process and historically targeted a 90 percent compliance threshold; however, this target has not been formally documented.

In addition, NCUA management stated that a process for monitoring the implementation of the baseline settings and remediating issues across all device platforms has not yet been finalized. As a result, devices, including Windows 11, Windows Server (b) (7)(E) Windows Server (b) (7)(E),

[14] Recommendation 4, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2025* (Report No. OIG-25-08, August 20, 2025).

(b) (7)(E) routers and switches, and (b) (7)(E) firewalls, reflected varying levels of baseline configuration compliance. The NCUA is in the process of implementing a new tool which will enable configuration of device level alerts to notify management when compliance falls below defined thresholds.

Furthermore, due to a planned migration of Windows Server (b) (7)(E) and (b) (7)(E) devices to Windows Server (b) (7)(E), the NCUA deferred remediation of certain baseline compliance issues until after the migration to the new operating system.

The NCUA *Configuration Management Control Family Document*, version 2.0, dated February 9, 2026, control CM-6, states the following regarding baseline configurations:

> * * *
> *b. Implement the configuration settings;*
> *c. Identify, document, and approve any deviations from established configuration settings for the information system components based on NCUA-defined operational requirements. NCUA-defined operational requirements are the minimum requirements that address the need of the organization.*

By consistently implementing secure baseline configurations, the NCUA can reduce the risk of unauthorized access to systems and sensitive data, as well as operational disruptions caused by weak configurations. In addition, maintaining and monitoring deviations from standard baseline configurations enhances the NCUA's ability to identify suspicious activity and prioritize remediation efforts. Furthermore, deploying devices with standardized baseline configurations enables the NCUA to troubleshoot issues and implement solutions more efficiently and effectively.

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

Recommendation 3: Develop and implement a baseline monitoring process that encompasses all devices in the environment. The process should define how baseline compliance is measured, establish the threshold at which a device is considered compliant with the approved baseline configuration, and specify the actions to be taken when a device is identified as noncompliant.

Agency Response:
NCUA agrees and will implement this recommendation by March 31, 2028.

OIG Response:
We acknowledge NCUA's concurrence with the recommendation.

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 5: *Optimized.* The NCUA has demonstrated strengths in this area by enforcing multi-

factor authentication for privileged and non-privileged users for applicable NCUA systems and implementing an enterprise-wide single sign-on solution that interfaces with its systems.

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.

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 2: *Defined*. Although the NCUA tailors specialized training to information security risks, the NCUA did not periodically update its workforce assessment of the skills, knowledge, and abilities of its cybersecurity professionals (refer to **Finding 3** below).

Finding 3: The NCUA did not periodically update its workforce assessment of the skills, knowledge, and abilities of its cybersecurity professionals to account for a changing risk environment.

The NCUA did not periodically update its workforce assessment of the skills, knowledge, and abilities of its cybersecurity professionals to account for a changing risk environment. The most recent cybersecurity workforce assessment was conducted in 2022.

The NCUA *Program Management Control Family Document* does not define the frequency for updating cybersecurity workforce assessments or describe the process for conducting them. As such, NCUA management stated that the NCUA does not have a documented process that defines how enterprise level cybersecurity workforce assessments should be conducted or how frequently they should be updated. As a result, the 2022 assessment remains the most recent one on record.

In addition, NCUA management stated that subsequent updates to the 2022 workforce assessment were deferred while the agency focused on other workforce management activities and operational priorities.

The NCUA *Program Management Control Family Document*, version 1.0, dated January 5, 2024, control PM-13, Security and Privacy Workforce, states that the NCUA is to establish a security and privacy workforce development and improvement program.

OMB Circular A-130, *Managing Information as a Strategic Resource*, dated July 28, 2016, Section 5. Policy, c. Leadership and Workforce, requires agencies to maintain a current workforce planning process to ensure that the agency can anticipate and respond to changing mission requirements and maintain workforce skills in a rapidly developing information technology environment.

Maintaining a current cybersecurity workforce assessment helps the NCUA identify missing or weak proficiencies across key cybersecurity domains, reducing the risk of security incidents occurring by addressing capability gaps. In addition, it enables targeted training ensuring teams have the necessary knowledge and abilities to respond to cybersecurity threats. Furthermore, it identifies whether people are performing functions aligned with their skills and knowledge and identifies where external skillsets may be required.

To assist the NCUA in periodically updating and maintaining a current cybersecurity workforce assessment, we recommend that NCUA management:

Recommendation 4: Update the *Program Management Control Family Document* to define the frequency for updating cybersecurity workforce assessments and document procedures to describe the process for conducting them.

Agency Response:
NCUA agrees and will implement this recommendation by September 30, 2026.

OIG Response:
We acknowledge NCUA's concurrence with the recommendation.

Recommendation 5: Update the cybersecurity workforce assessment in accordance with the documented procedures to maintain a current workforce planning process.

Agency Response:
NCUA agrees and will implement this recommendation by March 31, 2027.

OIG Response:
We acknowledge NCUA's concurrence with the recommendation.

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 4: *Managed and Measurable*.

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 4: *Managed and Measurable.* The NCUA has fully integrated its ISCM policies and strategy with its enterprise and supply chain 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 Event Logging (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 monitors and analyzes qualitative and quantitative performance measures on the effectiveness of its incident detection and analysis processes. In addition, the NCUA has implemented logging requirements at the EL3 (advanced) maturity level in accordance with OMB requirements.

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 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.

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 its systems and proactively employed procedures to disrupt systems and system components to more effectively test the effectiveness of its contingency planning processes.

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 the Federal Information Processing Standards issued by NIST. In addition, NIST develops and issues SPs as recommendations and guidance documents.

FISMA Reporting Requirements

The OMB and the DHS 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,* which provides reporting guidance for FISMA.[15] 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, CIGIE, and other stakeholders collaborated to develop these metrics.

As highlighted in **Table 2**, the 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: 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

CSF Functions	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance and Cybersecurity Supply Chain Risk Management
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.	Information Security Continuous Monitoring
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 IG FISMA Reporting Metrics

[15] See Footnote 1.

The foundational levels of the maturity model in the IG FISMA Reporting Metrics focus on 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 them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: 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 from October 1, 2025, through July 13, 2026. Within this period, we assessed the NCUA's information security program and practices' consistency with FISMA and reporting instructions issued by OMB and DHS for FY 2026. The scope of the audit also included assessing selected controls from NIST SP 800-53, Revision 5, supporting the IG FISMA Reporting Metrics for a sample of 4 of 67 NCUA-operated information systems and contractor-operated information systems in the NCUA's system inventory as of January 29, 2026 (**Table 4**).

Table 4: Description of Systems Selected for Testing

System	System Description
NCUA general support system (GSS) (NCUA-operated system)	The GSS provides the computing platform for all significant business applications of the NCUA. The platform includes all major information technology hardware, software, communications, network storage, central databases, operating systems, and other minor, infrastructure, security-related, and productivity applications.
Personnel Access and Security System (PASS) (NCUA-operated system)	PASS is a tool used to automate many of the processes the NCUA Office of Security and Continuity Management performs to record critical screening decisions, adjudicatory functions, and provide case management functions for the background investigations conducted on the NCUA employees and contractors.
USAi (contractor-operated system)	USAi is a multi-tenant generative artificial intelligence platform deployed in a Public Cloud model, hosted within the General Services Administration Federal Acquisition Service cloud environment on Amazon Web Services (AWS) cloud environment.
Tenable.io (contractor-operated system)	Tenable.io, is hosted on the AWS GovCloud infrastructure-as-a-service. Tenable.io, now known as Tenable Vulnerability Management, uses Tenable Nessus technology for scanning the NCUA's information system environment for vulnerabilities.

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.

The audit also included an evaluation of whether the NCUA took corrective actions to address open recommendations from the FY 2021,[16] FY 2024, [17] and FY 2025[18] FISMA audits. See **Appendix C** for the status of the prior-year recommendations.

The audit covered the period from October 1, 2025, through July 13, 2026. We performed audit fieldwork from March through July 2026.

[16] See Footnote 8.
[17] See Footnote 9.
[18] See Footnote 10.

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 FISMA reporting instructions that the OMB and the DHS issued.
- 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 the 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-operated and contractor-operated information systems from the 67 operational 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 14 NCUA-operated systems and 2 of the 53 contractor-operated systems for testing this year. All four systems selected for testing are designated as moderate-impact systems based on NIST Federal Information Processing Standard 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.

The *FY 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2026 FISMA audits. As part of this approach, core and supplemental IG FISMA Reporting Metrics were averaged 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, calculated averages were not automatically rounded 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 program and function-level effectiveness.

We used the IG FISMA Reporting Metrics guidance[19] 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.

[19] The 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 2021, FY 2024, and FY 2025 FISMA audits.[20] At the time of testing and IG FISMA Reporting Metric submission, all 13 prior-year recommendations from the audits referenced below were closed.

In the following table, the "Auditor's Position on Status" column is based on our inspection of evidence received during fieldwork. 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[21]
OIG-25-08 **Recommendation 1**	We recommend that NCUA management 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.	**Closed** We inspected evidence that NCUA documented 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.	Cybersecurity Governance
OIG-25-08 **Recommendation 2**	We recommend that NCUA management 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.	**Closed** We inspected evidence that NCUA created 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.	Cybersecurity Governance
OIG-25-08 **Recommendation 3**	We recommend that NCUA management 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.	**Closed** We inspected evidence that the NCUA updated 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.	Risk and Asset Management

[20] See Footnotes 8, 9, and 10.
[21] We mapped all prior-year recommendations to specific affected IG FISMA Reporting Metric domains based upon the nature of each recommendation.

Report No. Recommendation No.	Recommendation	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[21]
OIG-25-08 **Recommendation 4**	We recommend that NCUA management 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.	**Closed** We inspected evidence that the NCUA implemented baseline compliance monitoring for routers, switches, and firewalls on the NCUA network.	Configuration Management
OIG-25-08 **Recommendation 5**	We recommend that NCUA management 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.	**Closed** We inspected evidence that the NCUA improved 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.	Configuration Management
OIG-25-08 **Recommendation 6**	We recommend that NCUA management develop and implement procedures to remediate vulnerabilities for the third-party system within NCUA timeline requirements that fall outside of the vendor monthly patching schedule.	**Closed** We inspected evidence that the NCUA developed and implemented procedures to remediate vulnerabilities for the third-party system within NCUA timeline requirements that fall outside of the vendor monthly patching schedule.	Configuration Management
OIG-25-08 **Recommendation 7**	We recommend that NCUA management coordinate with the vendor to upgrade the third-party software or document any risk-based decisions, including compensating controls.	**Closed** We inspected evidence that the NCUA coordinated with the vendor to upgrade the third-party software.	Configuration Management
OIG-25-08 **Recommendation 8**	We recommend that NCUA management conduct a review of all current (b) (7)(E) (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.	**Closed** We inspected evidence that the NCUA conducted 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.	Identity and Access Management
OIG-25-08 **Recommendation 9**	We recommend that NCUA management validate that the NCUA completes quarterly account reviews for the (b) (7)(E) and (b) (7)(E) systems.	**Closed** We inspected evidence that the NCUA completed quarterly account reviews for the (b) (7)(E) and (b) (7)(E) systems.	Identity and Access Management

Report No. Recommendation No.	Recommendation	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains[21]
OIG-25-08 **Recommendation 10**	We recommend that NCUA management implement automatic disabling of privileged (b) (7)(E) user accounts upon 30 days of inactivity or document any risk-based decisions, including compensating controls.	**Closed** We inspected evidence that the NCUA implemented automatic disabling of privileged (b) (7)(E) user accounts upon 30 days of inactivity.	Identity and Access Management
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.	**Closed** We inspected evidence that the NCUA conducted refresher training for the PCs regarding documenting and maintaining asset management system records in accordance with NCUA policy and procedures.	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 information technology asset inventory to validate that the inventory is documented and maintained in accordance with NCUA policy and procedures.	**Closed** We inspected evidence that the NCUA updated the accountable property policy to implement a process for the PMO to complete a periodic review of the information technology asset inventory to validate that the inventory is documented and maintained in accordance with NCUA policy and procedures.	Risk and Asset Management
OIG-21-09 **Recommendation 1**	We recommend that the NCUA review the supply chain risk management (SCRM) NIST guidance and update the SCRM plan, policies, and procedures to fully address supply chain risk management controls and practices.	**Closed** We inspected evidence that the NCUA updated the SCRM plan, policies, and procedures to fully address NIST guidance regarding supply chain risk management controls and practices.	C-SCRM

Appendix D: Management Comments

NCUA

Memorandum

DATE: July 31, 2026

TO: Acting Inspector General Marta Erceg
Office of the Inspector General

FROM: Executive Director Larry Fazio
Office of the Executive Director

LARRY FAZIO Digitally signed by LARRY FAZIO Date: 2026.07.31 15:25:50 -04'00'

SUBJECT: FISMA Act of 2014 Fiscal Year 2026 Audit Draft Report

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) 2026*. The draft report concludes that NCUA has implemented an effective information security program, achieved an overall maturity level of Level 4 – *Managed and Measurable*, and complied with FISMA. NCUA's overall maturity level reflects its continuing commitment to strong information security.

The draft report makes five 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
Update the NCUA *Accountable Property Operations Handbook* to require documenting more granular location information (e.g., specific rooms or workspaces) for applicable asset types.

Management Response: NCUA agrees and will implement this recommendation by March 31, 2027.

Recommendation #2
Validate that the Property Management Officer completes periodic reviews of the asset management system data to confirm the inventory is documented and maintained in accordance with NCUA Instruction 1710.6 and the *Accountable Property Operations Handbook*.

Management Response: NCUA agrees and will implement this recommendation by March 31, 2027.

Recommendation #3

Develop and implement a baseline monitoring process that encompasses all devices in the environment. The process should define how baseline compliance is measured, establish the threshold at which a device is considered compliant with the approved baseline configuration, and specify the actions to be taken when a device is identified as noncompliant.

Management Response: NCUA agrees and will implement this recommendation by March 31, 2028.

Recommendation #4

Update the *Program Management Control Family Document* to define the frequency for updating cybersecurity workforce assessments and document procedures to describe the process for conducting them.

Management Response: NCUA agrees and will implement this recommendation by September 30, 2026.

Recommendation #5

Update the cybersecurity workforce assessment in accordance with the documented procedures to maintain a current workforce planning process.

Management Response: NCUA agrees and will implement this recommendation by March 31, 2027.

Please contact Acting Deputy Executive Director Kelly Lay if you have any questions.

Distribution:
Chairman Kyle Hauptman
Acting Chief of Staff Nate Kreoger
Acting Deputy Executive Director Kelly Lay
Acting Chief Information Officer Amber Gravius
Acting Deputy Chief Information Officer Dave Matheu
Cybersecurity Director Gidel Mendez

NCUA
National Credit Union Administration

Office of Inspector General

NCUA OIG
1775 Duke Street
Alexandria, VA 22314

The OIG's mission is to prevent, deter, and detect waste, fraud, abuse, and misconduct in NCUA programs and operations; and to promote economy, efficiency, and effectiveness at the agency.

To report allegations of waste, fraud, abuse, or misconduct regarding NCUA programs, employees, contractors, or contracts, please contact us via our OIG Hotline | NCUA or call 1-800-778-4806.

NCUA website | www.ncua.gov
Oversight.gov | www.oversight.gov

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.