NCUA
National Credit Union Administration

OFFICE OF INSPECTOR GENERAL

NATIONAL CREDIT UNION ADMINISTRATION FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT – FISCAL YEAR 2024

Report #OIG-24-08
September 12, 2024

SENT BY EMAIL

TO: Distribution List

THROUGH: Inspector General James W. Hagen

FROM: Deputy Inspector General R. William Bruns

SUBJECT: National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2024

DATE: September 12, 2024

Attached is the Office of Inspector General's FY 2024 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)[2] to perform this evaluation.[3] The contract required that this evaluation be 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.

This report summarizes the results of Sikich's independent evaluation and contains nine 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 a personal briefing, please contact me at 703-518-6350.

[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] Effective January 1, 2024, Sikich CPA LLC acquired CliftonLarsonAllen LLP's federal practice, including its work for the National Credit Union Administration Office of Inspector General.

[3] Sikich is an independent certified public accounting and consulting firm.

Distribution List:
Chairman Todd M. Harper
Board Vice Chairman Kyle S. Hauptman
Board Member Tanya Otsuka
Executive Director Larry Fazio
General Counsel Frank Kressman
Deputy Executive Director Rendell Jones
Chief of Staff Catherine Galicia
OEAC Deputy Director Samuel Schumach
Acting Chief Information Officer David Tillman
Deputy Chief Information Officer Rob Foster
Chief Financial Officer Eugene Schied
AMAC President Cory Phariss
E&I Director Kelly Lay
CURE Director Martha Ninichuk
OHR Director Towanda Brooks
OCSM Director Kelly Gibbs
OBI Director Amber Gravius
OCFP Director Matthew Biliouris
Cybersecurity Advisor and Coordinator Todd Finkler
Senior Agency Official for Privacy Linda Dent

Attachment

PERFORMANCE AUDIT OF THE NATIONAL CREDIT UNION ADMINISTRATION'S IMPLEMENTATION OF THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 FOR FISCAL YEAR 2024

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

PERFORMANCE AUDIT REPORT

SEPTEMBER 11, 2024

FINAL

ACCOUNTING TECHNOLOGY ADVISORY

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

SIKICH.COM

September 11, 2024

James Hagen
Inspector General
National Credit Union Administration

Dear Inspector General Hagen:

Sikich CPA LLC (Sikich)[1] 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 2024 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). FISMA requires federal agencies, including the NCUA, to perform an annual independent evaluation of their information security programs 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 NCUA Office of the Inspector General engaged Sikich to conduct this performance audit. The audit covered the period from October 1, 2023, through July 9, 2024. We performed the work from March through July 2024.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. These 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 further in **Appendix B: Objective, Scope, and Methodology**.

We appreciate the assistance provided by NCUA management and staff.

Sincerely,

Sikich CPA LLC

Alexandria, VA

[1] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's (CLA's) federal practice, including its work for the National Credit Union Administration Office of the Inspector General.

TABLE OF CONTENTS

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)[2] 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 NCUA's information security program and practices.

OMB and the Department of Homeland Security (DHS) annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*.[3] This memorandum describes the methodology for conducting FISMA audits and the process for federal agencies to report to OMB and, where applicable, DHS. According to that memorandum, each year the IGs are required to complete the IG FISMA Reporting Metrics[4] to independently assess their agency's information security program.

For this year's review, IGs were required to assess 20 core[5] and 17 supplemental[6] IG FISMA Reporting Metrics across five security function areas—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: *Managed and Measurable*. See **Appendix A** for additional 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 fiscal year (FY) 2024 IG FISMA reporting metrics, for a sample of 4 of the 63 NCUA-managed and third-party information systems[7] in the NCUA's system inventory as of

[2] Effective December 14, 2023, we amended our legal name from "Cotton & Company Assurance and Advisory, LLC" to "Sikich CPA LLC" (herein referred to as "Sikich"). Effective January 1, 2024, we acquired CliftonLarsonAllen LLP's (CLA's) federal practice, including its work for the NCUA OIG.
[3] See OMB Memorandum M-24-04 online here.
[4] See the Fiscal Year (FY) 2023 – 2024 IG FISMA Reporting Metrics online here. We provided the NCUA OIG with our responses to the FY 2024 IG FISMA Reporting Metrics as a separate deliverable under the contract for this audit.
[5] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine security program effectiveness.
[6] Supplemental metrics are assessed at least once every 2 years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.
[7] According to NIST, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

January 19, 2024. The audit covered the period from October 1, 2023, through July 9, 2024. We performed audit fieldwork from March through July 2024.

II. Summary of Results

We concluded that NCUA (1) implemented an effective information security program by achieving an overall maturity level 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 overall maturity levels for each security function and domain in the FY 2024 IG FISMA Reporting Metrics. We determined that three of the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) Function areas for the NCUA were at the Level 4: *Managed and Measurable* maturity level and two were at the Level 3: *Consistently Implemented* maturity level.

Table 1: Maturity Levels for FY 2024 IG FISMA Reporting Metrics

Maturity Level by Function	Domain	Maturity Level by Domain
Function: Identify		
Level 4: *Managed and Measurable*	Risk Management	Level 4: *Managed and Measurable* (Effective)
	Supply Chain Risk Management (SCRM)	Level 2: *Defined* (Not Effective)
Function: Protect		
Level 3: *Consistently Implemented*	Configuration Management	Level 3: *Consistently Implemented* (Not Effective)
	Identity and Access Management	Level 3: *Consistently Implemented* (Not Effective)
	Data Protection and Privacy	Level 5: *Optimized* (Effective)
	Security Training	Level 4: *Managed and Measurable* (Effective)
Function: Detect		
Level 4: *Managed and Measurable*	Information Security Continuous Monitoring (ISCM)	Level 4: *Managed and Measurable* (Effective)
Function: Respond		
Level 4: *Managed and Measurable*	Incident Response	Level 4: *Managed and Measurable* (Effective)
Function: Recover		
Level 3: *Consistently Implemented*	Contingency Planning	Level 3: *Consistently Implemented* (Not Effective)
Overall	**Level 4: *Managed and Measurable* (Effective)**	

Source: Sikich's assessment of the NCUA's information security program controls and practices based on the FY 2024 IG FISMA Reporting Metrics.

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.
- Continued to consistently implement its change control policies and procedures, including considering security impacts prior to implementing changes.

- Continued to integrate metrics on the effectiveness of its ISCM program to provide situational awareness across the organization.
- Implemented logging requirements at the Event Logging (EL) 1 maturity level (basic), in accordance with OMB requirements.[8]

Although we concluded that the NCUA implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We identified seven new weaknesses that fell in the Risk Management, SCRM, Configuration Management, Identity and Access Management, Security Training, and Contingency Planning domains of the FY 2024 IG FISMA Reporting Metrics, as follows:

- The NCUA did not maintain an up-to-date information technology (IT) asset inventory (Finding 1: Identify Function – Risk Management Domain).
- The NCUA did not consistently complete annual risk assessment reviews for all third-party NCUA services (Finding 2: Identify Function – Risk Management Domain).
- The NCUA did not consistently complete SCRM risk assessments for all third-party systems and service providers and has not fully completed SCRM policies and procedures (Finding 3: Identify Function – SCRM Domain).
- The NCUA did not consistently resolve network vulnerabilities within required timelines (Finding 4: Protect Function – Configuration Management Domain).
- The NCUA did not complete its backlog of overdue background reinvestigations (Finding 5: Protect Function – Identity and Access Management Domain).
- The NCUA did not ensure that all privileged users completed initial role-based security training in accordance with NCUA policy (Finding 6: Protect – Security Training Domain).
- NCUA has not completed its implementation of an alternate processing and storage site that is geographically separate from its primary site (Finding 7: Recover – Contingency Planning Domain).

In addition, the NCUA has outstanding prior-year recommendations that impact the IG FISMA Reporting Metrics. Specifically, at the beginning of FY 2024, NCUA had 14 open recommendations from prior FISMA audits for 2018,[9] 2019,[10] 2021,[11] 2022,[12] and 2023.[13] During our FY 2024 audit, we determined that the NCUA took corrective actions to address six of these recommendations, and we consider those recommendations closed. Corrective actions are in progress for the other eight open recommendations.[14] In addition, the NCUA has three

[8] OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, August 27, 2021, establishes a maturity model to guide the implementation of requirements across four EL tiers. Agencies were required to meet the EL1 maturity level by August 28, 2022.
[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] See Appendix C for the status of prior-year recommendations.

outstanding recommendations from a cybersecurity audit[15] 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, we made nine new recommendations to assist the NCUA in strengthening its information program. Additionally, we noted that eight prior-year recommendations remain open.[16]

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 of the audit. **Appendix C** provides the status of prior-year FISMA report recommendations. **Appendix D** includes management's comments.

III. 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's Cybersecurity Framework.

SECURITY FUNCTION: IDENTIFY

The objective of the Identify function is to develop an organizational understanding of the business context and the resources that support functions that are critical for managing cybersecurity risk to systems, people, assets, data, and capabilities. We determined that the maturity level of the NCUA's Identify function is Level 4: *Managed and Measurable*.

Risk Management

An agency with an effective risk 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 management program.

We determined that the maturity level of the NCUA's Risk Management domain is Level 4: *Managed and Measurable*. The NCUA continued to integrate cybersecurity risk management information into ERM reporting tools, and information security architecture is integrated with its systems development lifecycle. However, the NCUA did not maintain an up-to-date inventory of hardware assets and did not consistently perform system risk assessments in accordance with organization-defined timeframes.

[15] Recommendations 2, 3, and 4, *National Credit Union Administration Cybersecurity Audit* (Report No. OIG-23-05, May 2, 2023).
[16] See Appendix C for the status of prior-year recommendations.

Finding 1: The NCUA Did Not Maintain an Up-to-Date IT Asset Inventory.

As of March 6, 2024, the NCUA's IT asset inventory did not include all of the required data elements for 43 IT assets listed as "In Use." Specifically, the user's name or location were missing. These assets included items such as external hard drives, laptops, storage devices, routers, printers, and smartphones.

NCUA management indicated that the Property Custodian (PC) did not follow NCUA's policies and procedures regarding documenting the user's name and location in the inventory records. In addition, the Property Management Officer (PMO) did not effectively ensure that NCUA had correctly reported the accountable property in the inventory listing.

NIST SP 800-53, Revision 5*,* control CM-8, *System Component Inventory*, requires organizations to develop and document an inventory of system components that includes organization-defined information deemed necessary to achieve system component accountability at the level of granularity necessary for tracking and reporting.

The NCUA *Office of the Chief Financial Officer (OCFO) Accountable Property Operations Handbook*, dated September 6, 2019, Section 5.1, *Record Creation*, requires the PC to create an asset management system record for accountable property that meets the criteria for entry within 3 business days of receipt. The asset management system record must include (but is not limited to) the following data elements:

- Receipt Date
- Procurement Documentation Number
- Barcode Number
- Manufacturer
- Model Number
- Official Item Name (Description)
- Model Name
- Serial Number
- Initial Event (Assignment to NCUA employee, contractor staff, agency partner; or Replacement)
- Responsibility Date
- Effective Date
- Property Custodian Name
- User Name
- User Name Location:
    - Site (e.g., City, State)
    - Building (e.g., 1775 Duke Street)
    - Room Number/Cube Number

In addition, Section 6.1, *Location Reassignment, Internal Accountable Property Transfer, and Accountable Property Maintenance*, indicates that if an accountable property item changes location, needs to be reassigned to another person, or needs repair, the transferring PC is to update the record in the asset management system with data such as the new location, personnel, and property.

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.

By ensuring the system component inventory listing includes all required data fields, the NCUA would decrease its risk of lost or misplaced IT equipment and therefore also reduce the risk of data loss, including the loss of personally identifiable information.

To assist the NCUA with ensuring that it documents and maintains its IT asset inventory in accordance with NCUA policy, we recommend that NCUA management:

Recommendation 1: Conduct refresher training for the PCs regarding documenting and maintaining asset management system records in accordance with NCUA policy and procedures.

Agency Response:
The NCUA agrees with the recommendation. Property custodians will receive training on the policy and procedures concurrent with issuance of the revised *NCUA Instruction 1710.6, Receipt Transfer and Disposal of Accountable Property*, by June 30, 2025.

OIG Response:
We concur with management's specified action and will validate status during the FY 2025 FISMA audit.

Recommendation 2: 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.

Agency Response:
The NCUA agrees with the recommendation. The revised accountable property policy will be issued by June 30, 2025.

OIG Response:
We concur with management's specified action and will validate status during the FY 2025 FISMA audit.

Finding 2: The NCUA Did Not Consistently Complete Annual Risk Assessment Reviews for All Third-Party NCUA Services.

The NCUA did not perform an annual risk assessment review for the Delphi Procurement Request Information System Management (PRISM), one of the four systems selected for testing.

In January 2023, the Office of the Chief Information Officer (OCIO) transitioned oversight of the annual risk assessment reviews for all third-party NCUA services, other than those the OCIO

used, to another NCUA office. PRISM is one of the third-party services for which the OCIO transitioned oversight.

NCUA management indicated that it has experienced a delay in obtaining the security documentation needed to update the risk assessments from the vendors or service providers. Management specified that it is continuing to work on completing the reviews for these services.

NIST SP 800-53, Revision 5*,* control RA-3, *Risk Assessment*, requires organizations to review risk assessment results in accordance with the organization-defined frequency. Risk assessments must also consider risk from external parties, including contractors that operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.

The *NCUA Information Security Manual,* control RA-3, requires the NCUA to review its risk assessment results annually.

In addition, NIST SP 800-37, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*, Revision 2, states the following:

> *The authorization to use by the customer organization is a statement of the acceptance of risk in using the system, service, or application with respect to the customer's information.*
>
> *…*
>
> *The authorization to use does not require a termination date but remains in effect if the customer organization continues to accept the security and privacy risk of using the shared or cloud system, application, or service and the authorization to operate issued by the provider organization meets the requirements established by federal and organizational policies. It is incumbent on the customer organization to ensure that information from the monitoring activities conducted by the provider organization is shared on an ongoing basis and that the provider organization notifies the customer organization when there are significant changes to the system, application, or service that may affect the security and privacy posture of the provider.*

By assessing the risks associated with the use of external information systems, NCUA would increase its awareness of any risks inherent to the use of these systems. Furthermore, by adequately documented system risk assessments, the system owner and authorizing official would have the appropriate knowledge to mitigate known control weaknesses and make informed, risk-based decisions.

To assist the NCUA with consistently conducting annual system risk assessment reviews, we recommend that NCUA management:

Recommendation 3: Complete the PRISM risk assessment review on an annual basis and document the results.

Agency Response:
The NCUA agrees with the recommendation. The PRISM risk assessment will be complete by December 31, 2024.

OIG Response:
We concur with management's specified action and will validate completion during the FY 2025 FISMA audit.

Recommendation 4: Ensure that the annual risk assessment reviews for all third-party NCUA services are completed.

Agency Response:
The NCUA agrees with this recommendation. The NCUA has procedures in place to track third-party annual risk assessment reviews and monitors these assessments. NCUA will make necessary adjustments to improve the process and adhere to completion timeframes by March 31, 2025.

OIG Response:
We concur with management's specified action and will validate completion during the FY 2025 FISMA audit.

Supply Chain Risk Management

An agency with an effective SCRM program (1) ensures that external providers' products, system components, systems, and services are consistent with the agency's cybersecurity and SCRM requirements, and (2) reports qualitative and quantitative performance measures on the effectiveness of its SCRM program.

We determined that the maturity level of the NCUA's SCRM domain is Level 2*: Defined*. Specifically, we noted that the NCUA has not fully addressed the NIST 800-53 SCRM controls in its policies and procedures, nor has it completed its assessment of supply chain risks for all third-party systems and service providers.

Finding 3: The NCUA Did Not Consistently Complete SCRM Risk Assessments for All Third-Party Systems and Service Providers and Has Not Fully Completed SCRM Policies and Procedures.

The NCUA did not complete SCRM risk assessments for 90 percent (45 of 50) of the third-party systems listed in its information system inventory. In addition, the NCUA did not track 72 percent (36 of 50) of its third-party systems to verify whether it had completed the SCRM risk assessment. Finally, the NCUA has not defined and communicated its component authenticity[17] policies and procedures.

NCUA management stated that, because the NCUA has a limited number of licenses for its SCRM risk assessment tool, Prevalent, management prioritized tracking and completing risk assessments for those systems considered highest risk.

NCUA management also stated that the NCUA updated the SCRM-related clauses in the *NCUA Acquisition Policy Manual* (Revision 3) in December 2023. The updated manual requires contractors to mitigate supply chain risk and report any potential cyber-supply chain event. Through these clauses, the NCUA transferred operational responsibility for these risks and potential events, including responsibility for mitigating risks related to counterfeit components.

[17] Component authenticity controls are related to detecting and preventing counterfeit components from entering the NCUA information system environment.

Management therefore does not have policies or procedures in place related to anti-counterfeit measures and does not have a plan to develop separate policies and procedures.

However, there are components of NIST's anti-counterfeit controls for which the NCUA is still responsible and that the NCUA should therefore address in its policies and procedures. These controls include providing training on how to detect anti-counterfeit components and maintaining configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

NIST SP 800-53, Revision 5, control SR-6, *Supplier Assessments and Reviews*, requires the NCUA to assess and review the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide.

In addition, NIST SP 800-53, Revision 5, control SR-11, *Component Authenticity*, requires the NCUA to develop and implement anti-counterfeit policies and procedures that include the means to detect and prevent counterfeit components from entering the system.

By assessing the supply chain-related risks associated with third-party systems and service providers, the NCUA can identify potential threats and take action to mitigate them, enhancing business continuity and increasing security.

With developed and disseminated anti-counterfeit policies and procedures, NCUA personnel can better identify and reduce the risk of introducing counterfeit components into the NCUA's information system environment.

The FY 2021 NCUA FISMA report identified SCRM controls that the NCUA had not addressed in its policies and procedures, including controls related to detecting and preventing the deployment of counterfeit components. The report recommended that the NCUA review the NIST guidance related to SCRM and update its SCRM plan, policies, and procedures to fully address SCRM controls and practices.[18] We are therefore not making a new recommendation regarding anti-counterfeit policies and procedures.

To assist the NCUA with completing its assessment of supply chain risks for all third-party systems and service providers, we recommend that NCUA management:

Recommendation 5: Document and implement a process to track and complete supply chain risk assessments for all third-party systems and service providers.

Agency Response:
The NCUA agrees with this recommendation. The NCUA is implementing a new solution that will allow for full coverage of all third-party vendors and will complete the risk assessments by December 31, 2025.

OIG Response:
We concur with management's specified action and will validate status during the FY 2025 FISMA audit.

[18] Recommendation 1, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2021 Report*, #OIG-21-09, November 22, 2021.

SECURITY FUNCTION: PROTECT

The objective of the Protect function is to develop and implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event. 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; consistently implements its configuration management policies, procedures, plans, and strategy at all levels of the organization; 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 3: *Consistently Implemented.* The NCUA has demonstrated strengths in this area by consistently implementing its change control policies and procedures, including considering security impacts prior to implementing changes.

However, we identified areas for improvement in the NCUA's vulnerability management program and noted that the NCUA has four open prior-year recommendations in the Configuration Management domain[19] that relate to improving its vulnerability management program[20] [21] and implementing standard baseline configurations.[22] We conducted independent vulnerability scans during the FY 2024 FISMA audit and identified similar issues related to vulnerability management.

Finding 4: The NCUA Did Not Consistently Resolve Network Vulnerabilities Within Required Timelines.

Using vulnerability data from the Common Vulnerability Scoring System (CVSS[23]) used by the vulnerability scanning tool Nessus, we identified unpatched software, unsupported software, and improper configuration settings that exposed the NCUA network to critical[24] and high[25]-severity vulnerabilities.

[19] See Appendix C for additional information regarding these prior-year recommendations.
[20] 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).
[21] 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).
[22] 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).
[23] CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its 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.
[24] The critical rating is based on the CVSS, which provides a standardized way of reporting vulnerabilities by the risk they pose to an organization. Critical vulnerabilities possess a rating of 10.
[25] High-risk vulnerabilities possess a CVSS rating of 7 to 9.9.

The NCUA did not resolve critical vulnerabilities within 30 days of occurrence and high-risk vulnerabilities within 60 days of occurrence, as required by its internal operating policies. Furthermore, the NCUA did not timely remediate older vulnerabilities that became publicly known before January 2024.

The credential scans of 401 hosts identified 159 total instances comprised of 57 unique critical and high-risk vulnerabilities related to patch management, configuration management, and unsupported software that fell outside of the NCUA's remediation timeframe.[26] Of the vulnerabilities identified, the NCUA did not remediate 9 percent of critical vulnerabilities (5 of 54) and 59 percent of high-risk vulnerabilities (62 of 105) in accordance with the NCUA's defined patching timeframes. Some of these vulnerabilities included:

- (b) (7)(E) [redacted]

Furthermore, the credentialed scans identified 22 vulnerabilities that the NCUA was required to patch in accordance with the Cybersecurity & Infrastructure Security Agency's (CISA's)[27] Known Exploitable Vulnerability (KEV) listing.[28] Due dates for the past-due KEVs ranged from December 24, 2021, through October 21, 2023.

NCUA management stated that the NCUA is not leveraging dashboards to monitor patch and vulnerability compliance and track approved and unapproved software. In addition, the NCUA has not adequately defined, implemented, monitored, and managed its patch management workflow to ensure that it installs patches in accordance with the required timelines.

NIST SP 800-53, Revision 5, control SI-2, *Flaw Remediation*, requires organizations to install security-relevant software and firmware updates within an organization-defined time period of the release of the updates.

The *NCUA Information Systems Security Manual,* Control Risk Assessment (RA)-5, *Vulnerability Scanning*, specifies the following response times for remediating vulnerabilities:

- *Internal-Facing Assets: Critical – 30 days from discovery, High – 60 days from discovery, Medium – 90 days from discovery, and Low as time permits in accordance with an organizational assessment of risk.*

In addition, OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix I, states that:

[26] For comparison, the 2023 auditor credential scans of 304 hosts identified 375 total instances comprised of 69 unique critical and high-risk vulnerabilities that fell outside the NCUA's remediation timeframe.
[27] CISA, a component of DHS, is responsible for cybersecurity and infrastructure protection for all levels of government.
[28] 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.

- *Agencies are to implement and maintain current updates and patches for all software and firmware components of information systems; and*
- *Agencies are to prohibit the use of unsupported information systems and system components and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement.*

CISA Binding Operation Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*, states that agencies are required to remediate each vulnerability according to 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 remediate vulnerabilities within 6 months for vulnerabilities with a Common Vulnerabilities and Exposures (CVE)[29] 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 installing required patches, implementing secure configuration settings, and migrating to supported software, the NCUA can mitigate its security weaknesses and limit the potential for attackers to compromise the confidentiality, integrity, and availability of sensitive credit union and employee data. This will ultimately improve the overall security posture of the NCUA's information systems.

We conducted vulnerability scans during 2018 and made two recommendations related to remediating patch and configuration-related vulnerabilities within agency-defined timeframes and implementing a process to migrate unsupported software to supported platforms before support for the software ends.[30] We conducted additional scans in 2020, 2021, 2022, and 2023 with similar results. In 2022, we made additional recommendations related to developing a staffing plan to allocate appropriate and sufficient resources to improve the OCIO's ability to remediate persistent vulnerabilities and develop a plan to reduce the wide variety of differing technologies requiring support and vulnerability remediation, as feasible.[31] Except for the recommendation related to a staffing plan, all of these prior recommendations remain open.[32]

To further assist the NCUA in strengthening its vulnerability management process, we recommend that NCUA management:

Recommendation 6: 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.

Agency Response:
The NCUA agrees with this recommendation. The NCUA will implement an improved process for monitoring and managing this area by March 31, 2025.

OIG Response:
We concur with management's specified action and will validate completion during the FY 2025 FISMA audit.

[29] CVE is a list of all publicly known vulnerabilities that include the CVE ID.
[30] See Footnote 20.
[31] Recommendations 2 and 3, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (Report No. OIG-22-07, October 26, 2022).
[32] See Appendix C for the status of prior-year recommendations.

Identity and Access Management

An agency with an effective identity and access management program ensures that all privileged and non-privileged users use strong authentication for accessing organizational systems; employs automated mechanisms to support the management of privileged accounts; and monitors, analyzes, and reports qualitative and quantitative performance measures on the effectiveness of its identity, credential, and access management program.

We determined that the maturity level of the NCUA's Identity and Access Management domain is Level 3: *Consistently Implemented.* The NCUA has demonstrated strengths in this area by enforcing multi-factor authentication for non-privileged users and by periodically recertifying privileged user access rights.

However, we determined that the NCUA has opportunities to improve its identity and access management program by implementing the two open prior-year recommendations in this area.[33] These recommendations relate to implementing a solution that resolves a privileged access management vulnerability[34] and 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.[35] In addition, during the current year we noted a control weakness related to overdue background reinvestigations.

Finding 5: The NCUA Did Not Complete Its Backlog of Overdue Background Reinvestigations.

Based on our review of the Office of Continuity and Security Management (OCSM) background investigation listing of personnel that require background investigations, as of May 20, 2024, we determined that 9.5 percent (115 out of 1,211)[36] individuals (including employees and contractors) had overdue background reinvestigations. Specifically, we noted the following overdue background reinvestigations (broken down by background investigation tier):

- **Tier 2:**[37] 8.5 percent (59 out of 693) individuals had not undergone a background reinvestigation within the past 5 years, as the Office of Personnel Management (OPM) requires.
- **Tier 4:**[38] 11.5 percent (53 out of 461) individuals had not undergone a background reinvestigation within the past 5 years, as OPM requires.
- **Tier 5:**[39] 5.4 percent (3 out of 56) individuals had not undergone a background reinvestigation within the past 5 years, as OPM requires.

[33] See Appendix C for additional information regarding these prior-year recommendations.
[34] 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).
[35] 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).
[36] The discrepancy between the 1,211 total individuals requiring background investigations and the 1,210 identified in the tier-level breakdown occurred because one individual required a Tier 3-level background investigation that was not overdue.
[37] A Tier 2 investigation applies to moderate-risk positions in non-sensitive public trust roles. Public trust positions involve duties with a certain level of program responsibility and a significant degree of trust.
[38] A Tier 4 investigation applies to high-risk positions in non-sensitive public trust roles.
[39] A Tier 5 investigation applies to high-risk national security positions that require access to non-critical sensitive, special sensitive, or critical sensitive information.

In 2023 and 2024, NCUA management had issues with funding allocation and invoicing with the Defense Counterintelligence and Security Agency (DCSA).[40] The funding document was signed and executed in late January 2024, however; there were persistent errors with DCSA invoices and delays in updating the DCSA financial systems to correct the issues. As such, management prioritized completing new-hire investigations required for onboarding and postponed reinvestigations to prevent invoicing issues.

OPM's regulation at Title 5 Code of Federal Regulations (CFR) part 731.106 requires agencies to submit and adjudicate public trust reinvestigations at least once every 5 years.

NIST SP 800-53, Revision 5, control PS-3, *Personnel Screening*, requires organizations to rescreen individuals in accordance with organization-defined conditions, including the frequency of rescreening.

The *NCUA Information Security Manual,* published August 4, 2023*,* control PS-3, requires the NCUA to rescreen individuals in accordance with OPM suitability standards and the Office of the Director of National Intelligence's security standards regarding periodic reinvestigations and continuous evaluations.

By rescreening its employees, the NCUA can revalidate that individuals remain suitable for the level of system access or job responsibilities assigned to them. Ultimately, this helps protect the confidentiality, integrity, and availability of the NCUA's data and systems.

To assist the NCUA with consistently rescreening personnel, we recommend that NCUA management:

Recommendation 7: Complete the 2024 backlog of overdue reinvestigations.

Agency Response:
The NCUA agrees with this recommendation. Reinvestigations, as required, will be completed by December 31, 2024.

OIG Response:
We concur with management's specified action and will validate completion during the FY 2025 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 5: *Optimized.* The NCUA has demonstrated strengths in this area by integrating its data breach response plan with incident response, risk management, and continuous monitoring. In addition, the NCUA has integrated network defenses into its ISCM and incident response

[40] DCSA is the largest investigative service provider in the federal government conducting background investigations, continuous vetting, and adjudications.

programs to provide near real-time monitoring of the data that is entering and exiting the network, as well as other suspicious inbound and outbound communications.

However, we determined that the NCUA has opportunities to improve its data protection and privacy program by implementing the open prior-year recommendation associated with a FY 2023 supplemental metric related to implementing media marking.[41]

Security Training

An agency with an effective security training program identifies and addresses gaps in security knowledge, skills, and abilities; measures the effectiveness of its security awareness and training program; and ensures that staff consistently collect, monitor, and analyze qualitative and quantitative performance measures on the effectiveness of security awareness and training activities.

We determined that the maturity level for the NCUA's Security Training domain is Level 4: *Management and Measurable*. Although we determined that the Security Training domain was effective, we noted a control weakness related to role-based security training for privileged users.

Finding 6: The NCUA Did Not Ensure That All Privileged Users Completed Initial Role-Based Security Training in Accordance With NCUA Policy.

We determined that none of the three sampled privileged users (from a total population of nine) completed initial role-based security training within 60 days of being granted system access.

NCUA management indicated that the NCUA did not have a process in place to notify the Office of Human Resources (OHR) to add the initial role-based security training requirement to an individual's learning profile in the learning management system.

The *NCUA Information Security Manual,* published August 4, 2023*,* control Awareness and Training (AT-3), *Role-Based Training*, requires providing role-based security training within 60 days of being granted access to the system, information, or performing assigned duties based on Workforce Framework for Cybersecurity (NICE Framework)[42] categories and otherwise at the discretion of the Senior Agency Information Security/Risk Officer and the Senior Agency Official for Privacy.

By completing initial role-based security training, new personnel will be aware of their roles and responsibilities, as well as NCUA-specific information security requirements, tools, and methods. Additionally, role-based training helps ensure NCUA personnel are trained in the specific skills needed to perform their roles and responsibilities.

To assist the NCUA with consistently completing initial role-based security training, we recommend that NCUA management:

[41] 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).
[42] The NICE framework describes the knowledge and skills needed to perform cybersecurity work and enables organizations to develop their workforces to perform such work.

Recommendation 8: Document and implement a process for notifying 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.

Agency Response:
The NCUA agrees with this recommendation. NCUA will document and implement a process to notify OHR to add the initial role-based security training to the learning profile of new hires that are privileged users by December 31, 2024.

OIG Response:
We concur with management's specified action and will validate completion during the FY 2025 FISMA audit.

SECURITY FUNCTION: DETECT

The objective of the Detect function is to implement continuous monitoring of control activities to discover and identify cybersecurity events in a timely manner. Cybersecurity events[43] include anomalies and changes in the organization's IT environment that may impact organizational operations, including mission, capabilities, or reputation. We determined that the maturity level of the NCUA's Detect function is Level 4*: Managed and Measurable.*

Information Security Continuous Monitoring (ISCM)

An agency with an effective ISCM program maintains ongoing authorizations of information systems; integrates metrics on the effectiveness of its ISCM program in delivering persistent situational awareness across the organization; 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 demonstrated strengths in this area by integrating metrics on the effectiveness of its ISCM program to deliver persistent situational awareness across the organization and using the results of security control assessments and monitoring to maintain information system authorization.

SECURITY FUNCTION: RESPOND

The objective of the Respond function is to implement processes to contain the impact of detected cybersecurity events. Such processes include developing and implementing incident response plans and procedures, analyzing security events, and effectively communicating incident response activities. 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.

[43] According to NIST, a cybersecurity event is a cybersecurity change that may have an impact on organizational operations (including mission, capabilities, or reputation). See https://csrc.nist.gov/glossary/term/cybersecurity_event.

- 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.

We determined that the maturity level of the NCUA's Incident Response domain is Level 4: *Managed and Measurable.* The NCUA implemented logging requirements at the EL1 maturity level (basic), in accordance with OMB requirements, and it uses incident response metrics to measure and manage the timely reporting of incident information to the U.S. Computer Emergency Readiness Team.[44]

However, the NCUA has open recommendations in this area related to implementing requirements across the EL2 and EL3 maturity levels to ensure that it logs and tracks events in accordance with OMB Memorandum M-21-31.[45] Completing these logging requirements will assist the NCUA in continuing to strengthen its incident response capabilities.

SECURITY FUNCTION: RECOVER

The objective of the Recover function is to develop and implement activities to maintain plans for resilience and to restore capabilities or services impaired due to a cybersecurity incident. The Recover function supports the timely recovery of normal operations to reduce the impact of a cybersecurity incident, including recovery planning, improvements, and communications.

We determined that the maturity level of the NCUA's Recover function is Level 3: *Consistently Implemented*.

Contingency Planning

An agency with an effective contingency planning program establishes contingency plans; employs automated mechanisms to thoroughly and effectively test system contingency plans; communicates metrics on the effectiveness of recovery activities to relevant stakeholders; and consistently collects, monitors, and analyzes qualitative and quantitative performance measures regarding the effectiveness of information system contingency planning program activities.

We determined that the maturity level for the NCUA's Contingency Planning domain is Level 3: *Consistently Implemented.* The NCUA has consistently developed and implemented information system contingency plans and tested those plans in accordance with NCUA policies and procedures. However, we noted a control weakness related to the alternate processing and storage site.

[44] U.S. CERT, a component of DHS is responsible for analyzing and reducing cyber threats and vulnerabilities, disseminating cyber threat warning information, and coordinating incident response activities.
[45] See footnote 15.

Finding 7: The NCUA Has Not Completed the Implementation of an Alternate Processing and Storage Site That Is Geographically Separate From the Primary Site.

The NCUA alternate processing and storage site is not sufficiently geographically separated from the primary site to reduce susceptibility to the same external threats. The alternate site is located only 30 miles from the primary site, in the same metropolitan area.

The NCUA's alternate processing and storage site was previously located in a facility hosted by the Federal Reserve Board (FRB) in Richmond, Virginia. On July 29th, 2022, the FRB notified the NCUA that the warm site would no longer be available after December 31, 2023, due to the lease not being renewed. On November 15, 2023, the NCUA temporarily moved partial Disaster Recovery (DR) functions to the NCUA Central Office in Alexandria, Virginia, until the NCUA was able to fully migrate its functions to a geographically dispersed permanent site.

The NCUA began preparing to select a new DR site on July 29, 2022. It selected a new site in Phoenix, Arizona, on August 1, 2023. Infrastructure services are scheduled to be completed on July 31, 2024, and alternative processing and storage will be in partial production on January 31, 2025. NCUA management was not able to provide a date when the new site will be fully operational.

NIST SP 800-53, Revision 5, controls CP-6, *Alternate Storage Site*, and CP-7, *Alternate Processing Site*, control enhancement 1, require the NCUA to identify an alternate processing and storage site that is sufficiently separated from the primary processing site to reduce susceptibility to the same threats.

With an alternate processing and storage site that is geographically distinct and separate from the primary site, the NCUA would reduce the risk that its processing and storage of data would be affected should the primary site become unavailable due to the same external threat. Ultimately, geographically distinct and separate sites will reduce the risk that the NCUA does not lose critical data and that mission-critical activities continue in the event of a disruption or outage at the primary site.

To assist the NCUA with reducing the risk associated with its alternate processing and storage site, we recommend that NCUA management:

Recommendation 9: Complete implementation of the new alternate processing and storage site to a fully operational state.

Agency Response:
The NCUA agrees with this recommendation. While the NCUA will make substantial progress on this project by December 31, 2024, complete fail-over processing and storage services will be implemented by December 31, 2025.

OIG Response:
We concur with management's specified action and will validate status during the FY 2025 FISMA audit.

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 FIPS issued by NIST. In addition, NIST develops and issues SPs as recommendation and guidance documents.

FISMA Reporting Requirements

OMB and DHS annually provide federal agencies and IGs with instructions for preparing FISMA reports. On December 4, 2023, OMB issued Memorandum M-24-04, *Fiscal Year 2024 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the methodology for conducting FISMA evaluations and the processes for federal agencies to report to OMB and, where applicable, DHS. The methodology includes the following:

- OMB selected 17 supplemental IG FISMA Reporting Metrics that IGs must evaluate during FY 2024, in addition to the 20 core IG FISMA Reporting Metrics that IGs must evaluate annually. The remainder of the standards and controls are evaluated on a 2-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. Beginning in FY 2023, ratings were focused on calculated average scores, wherein IGs would use the average of the metrics in a particular domain to determine the effectiveness of the individual function areas (i.e., Identify, Protect, Detect, Respond, and Recover). OMB encouraged IGs to focus on the calculated average scores of the 20 core IG FISMA Reporting Metrics, as these tie directly to the administration's priorities and other high-risk areas. In addition, the FY 2024 IG FISMA Reporting Metrics indicated that IGs should use the calculated average scores of the supplemental IG FISMA Reporting Metrics and the agency's progress in addressing outstanding prior-year recommendations as data points to support their risk-based determination of the overall effectiveness of the program and function level.

As highlighted in **Table 2**, the IG FISMA Reporting Metrics are designed to assess the maturity of the information security program and align with the five functional areas in the NIST Cybersecurity Framework, version 1.1: Identify, Protect, Detect, Respond, and Recover.

Table 2: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2024 IG FISMA Reporting Metrics

Cybersecurity Framework Function Area	Function Area Objective	Domain(s)
Identify	Develop an organizational understanding of the business context and the resources that support critical functions to manage cybersecurity risk to systems, people, assets, data, and capabilities.	**Risk Management and SCRM**
Protect	Implement safeguards to ensure delivery of critical infrastructure services, as well as to prevent, limit, or contain the impact of a cybersecurity event.	**Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training**
Detect	Implement activities to identify the occurrence of cybersecurity events.	**ISCM**
Respond	Implement processes to take action regarding a detected cybersecurity event.	**Incident Response**
Recover	Implement plans for resilience to restore capabilities or services impaired by a cybersecurity event.	**Contingency Planning**

Source: Sikich's analysis of the NIST Cybersecurity Framework and 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 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, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2024 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

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards, issued by the Comptroller General of the United States. These 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.

The scope of this performance audit covered the NCUA's information security program and practices consistent with FISMA and reporting instructions that OMB and DHS issued for FY 2024. The scope also included assessing selected controls from NIST SP 800-53, Revision 5, to support the FY 2024 IG FISMA Reporting Metrics for a sample of 4 of 63 NCUA-managed and third-party information systems in the NCUA's system inventory as of January 19, 2024, as described in 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.
Consumer Access Process and Reporting Information System (CAPRIS) (NCUA-managed system)	CAPRIS replaced the Insurance Information System, which was composed of two distinct but related applications: the Generated Efficient National Information System for Insurance Services and the Field of Membership Internet Application. CAPRIS combined the functionality of the two applications, which includes capabilities to provide user entry screens to input and manage various credit union structure functions and events, and to generate national and regional-specific reports. CAPRIS resides in the NCUA data center.
Delphi Procurement Request Information System Management (PRISM) (third-party system)	PRISM is a customized Oracle commercial-off-the-shelf procurement system owned by the Department of Transportation, Federal Aviation Administration (FAA), and is maintained/operated by the FAA's Enterprise Services Center division. The NCUA uses PRISM as an acquisition and comprehensive procurement system and a data repository system that allows users to search, browse, maintain, share, classify, register, and standardize procurement-related items through PRISM's front-facing web application.
Archer Governance, Risk, and Compliance (GRC) (third-party system)	The RSA Archer Hosting Services is a multi-tenant, community cloud offering leveraging hardware infrastructure components to provide business-level management solutions for enterprise governance, risk, and compliance.

Source: NCUA System Inventory

The audit also included an evaluation of whether the NCUA took corrective actions to address open recommendations from the FY 2018 FISMA audit,[46] FY 2019 FISMA audit,[47] FY 2021 FISMA audit,[48] FY 2022 FISMA audit,[49] and FY 2023 FISMA audit.[50]

The audit covered the period from October 1, 2023, through July 9, 2024. We performed audit fieldwork from March through July 2024.

Methodology

To accomplish our 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 OMB and DHS issued for FY 2024.
- Focused our testing activities on assessing the maturity of the 20 core and 17 supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Inquired of NCUA management and staff.
- Considered guidance contained in OMB's Memorandum M-24-04, *Fiscal Year 2024 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 63 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 information systems and selected 2 of the 13 NCUA-managed systems and 2 of the 50 third-party systems for testing this year. The General Support System (GSS), PRISM, and Archer are designated as moderate-impact systems, and CAPRIS is designated as a low-impact system, 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.
- Reviewed results from other related NCUA OIG reports.

The FY 2023 IG FISMA Reporting Metrics introduced a calculated average scoring model that was continued for the FY 2024 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, calculated averages were not automatically

[46] See Footnote 9.
[47] See Footnote 10.
[48] See Footnote 11.
[49] See Footnote 12.
[50] See Footnote13.

rounded to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, 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. 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 2024 IG FISMA Reporting Metrics guidance[51] to form our conclusions for each Cybersecurity Framework 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.

We evaluated the effectiveness of the NCUA's information security program and practices, including with regard to FISMA and related information security policies, procedures, standards, and guidelines, and responded to the FY 2024 IG FISMA Reporting Metrics. 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.

[51] The FY 2024 IG FISMA Reporting Metrics provided the agency IG with the discretion to determine the rating for each of the Cybersecurity Framework 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's 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, FY 2019, FY 2021, FY 2022, and FY 2023 FISMA audits.[52] At the time of testing and IG FISMA Reporting Metric submission, 8 of the 14 prior-year recommendations from the audits referenced above remained open.

In the following table, the "NCUA's Status" column summarizes the information that NCUA management provided regarding the status of the prior-year recommendations. 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	NCUA's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
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.	This recommendation is open. Estimated target completion date: June 30, 2025	Open We inquired with NCUA personnel and learned that the NCUA has not updated the active script to dynamically identify new servers.	**Identity and Access Management**
OIG-23-08 **Recommendation 2**	We recommend that NCUA management validate that the onboarding workflow is working properly between SharePoint and LAMP to ensure that new employees and contractors are completing the NCUA Rules of Behavior timely upon onboarding.	The NCUA considers this recommendation to be fully remediated and requested closure of this recommendation.	Closed We inquired with NCUA personnel and learned that LAMP is no longer integrated with SharePoint. Users are organized through a dynamic grouping process in which they are automatically placed into new hire groups and assigned training. New hires acknowledge the Rules of Behavior via the new hire security awareness training. We inspected screenshots showing that users are dynamically assigned into groups.	**Identity and Access Management**
OIG-22-07 **Recommendation 1**	We recommend that NCUA enforce the process to validate that expired MOUs [Memoranda of	The NCUA considers this recommendation to be fully remediated and requested	Closed	**Risk Management**

[52] See Footnotes 9, 10, 11, 12, and 13.

Report No. Recommendation No.	Recommendation	NCUA's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	Understanding] and those expiring are prioritized for review, update, and renewal in accordance with NCUA policy.	closure of this recommendation.	We inspected evidence supporting that the NCUA had implemented an automated workflow with notifications to track upcoming MOU expirations and automated dashboards that track the interconnected system, status, MOU/Interconnection Security Agreement expiration date, date of agreement, and any status discrepancies.	
OIG-22-07 **Recommendation 2**	We recommend that NCUA conduct a workload analysis within OCIO and document a staffing plan to allocate appropriate and sufficient resources to improve OCIO's ability to perform remediation of persistent vulnerabilities caused by missing patches, configuration weaknesses, and outdated software.	The NCUA considers this recommendation to be fully remediated and requested closure of this recommendation.	Closed We inspected evidence detailing that the FY 2023 NCUA budget included four additional cybersecurity positions, two of which would focus on vulnerability management.	**Configuration Management**
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.	The NCUA considered this recommendation to be fully remediated and requested closure of this recommendation. Upon our determination that the recommendation was not closed, the NCUA provided an updated estimated target completion date. Estimated target completion date: June 30, 2025	Open We obtained the newly formed Technical Review Board Charter and meeting minutes from the meetings in January 2024 and April 2024. Neither set of meeting minutes evidenced that the NCUA had performed an analysis of technologies employed within the NCUA. In addition, the NCUA was unable to provide evidence to support that it had developed a plan to reduce the wide variety of differing technologies.	**Configuration Management**
OIG-22-07 **Recommendation 4**	We recommend that NCUA implement a solution that resolves the privileged access management vulnerability.	The expected completion date was December 2023; however, the NCUA was unable to complete remediation in the specified period. Management provided a new expected	Open Our testing during fieldwork indicated that the NCUA has not resolved the privileged access management issue.	**Identity and Access Management**

Report No. Recommendation No.	Recommendation	NCUA's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
		completion date of June 30, 2025.		
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.	The NCUA considers this recommendation to be fully remediated and requested closure of this recommendation.	Open Our testing during fieldwork indicated that the NCUA has not defined and communicated its component authenticity policies and procedures in accordance with NIST requirements. See Finding 3.	**Supply Chain Risk Management**
OIG-21-09 **Recommendation 2**	We recommend that NCUA document and implement a plan to deploy multifactor authentication to address increased risks with the large number of personnel teleworking without a PIV card during the pandemic.	The NCUA considers this recommendation to be fully remediated and requested closure of this recommendation.	Closed Our testing during fieldwork indicated that the NCUA has consistently implemented multifactor authentication for non-privileged users.	**Identity and Access Management**
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.	This recommendation is open. Estimated target completion date: FY 2024, Quarter (Q) 4	Open We inquired with NCUA personnel regarding open prior-year recommendations and determined that corrective action is ongoing.	**Data Protection and Privacy**
OIG-21-09 **Recommendation 7**	We recommend that NCUA select and implement a tool for file integrity monitoring.	The NCUA considers this recommendation to be fully remediated and requested closure of this recommendation.	Closed Our testing during fieldwork indicated that the NCUA has implemented a tool for file integrity monitoring.	**Configuration Management**
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	This recommendation is open. Estimated target completion date: December 31, 2024	Open We inquired with NCUA personnel regarding open prior-year recommendations and determined that corrective action is ongoing.	**Configuration Management**

Report No. Recommendation No.	Recommendation	NCUA's Status	Auditor's Position on Status	Affected IG FISMA Reporting Metric Domains
	from the configuration baselines with business justifications.			
OIG-18-07 **Recommendation 8**	We recommend that NCUA enforce the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.	This recommendation is open. Estimated target completion date: June 30, 2025	Open Our testing during fieldwork noted unpatched software, unsupported software, and improper configuration settings that exposed the NCUA Headquarters network to critical and high-severity vulnerabilities. See Finding 4.	**Configuration Management**
OIG-18-07 **Recommendation 9**	We recommend that NCUA implement a process to detect and migrate unsupported software to supported platforms before support for the software ends.	This recommendation is open. Estimated target completion date: June 30, 2025	Open Our testing during fieldwork identified unsupported software on the NCUA Headquarters network. See Finding 4.	**Configuration Management**
OIG-18-07 **Recommendation 10**	We recommend that NCUA implement a process to identify authorized software in its environment and remove any unauthorized software.	The NCUA considers this recommendation to be fully remediated and requested closure of this recommendation.	Closed Our testing during fieldwork determined that the NCUA implemented an automated rule to detect when privileged users install software. Non-privileged users are not able to install software. Upon detection, the NCUA removes the unauthorized software.	**Risk Management**

APPENDIX D: MANAGEMENT COMMENTS

NATIONAL CREDIT UNION ADMINISTRATION
Office of the Executive Director

SENT BY EMAIL

TO: Inspector General James W. Hagen

FROM: Deputy Executive Director Rendell L. Jones Digitally signed by RENDELL JONES
Date: 2024.08.28
13:17:55 -04'00'

SUBJ: Draft Report for Federal Information Security Modernization Act of 2014 Audit Fiscal Year 2024

DATE: August 28, 2024

Thank you for the opportunity to review and comment on the draft report for the *Federal Information Security Modernization Act of 2014 (FISMA) Audit Fiscal Year (FY) 2024*. The draft report concludes that the NCUA 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 the NCUA's commitment to strong information security practices.

The draft report makes nine 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
Conduct refresher training for the PCs [property custodians] regarding documenting and maintaining asset management system records in accordance with NCUA policy and procedures.

Management Response: The NCUA agrees with the recommendation. Property custodians will receive training on the policy and procedures concurrent with issuance of the revised *NCUA Instruction 1710.6, Receipt Transfer and Disposal of Accountable Property*, by June 30, 2025.

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

Management Response: The NCUA agrees with the recommendation. The revised accountable property policy will be issued by June 30, 2025.

Recommendation #3
Complete the PRISM risk assessment review on an annual basis and document the results.

Management Response: The NCUA agrees with the recommendation. The PRISM risk assessment will be complete by December 31, 2024.

Recommendation #4
Ensure that the annual risk assessment reviews for all third-party NCUA services are completed.

Management Response: The NCUA agrees with this recommendation. The NCUA has procedures in place to track third-party annual risk assessment reviews and monitors these assessments. NCUA will make necessary adjustments to improve the process and adhere to completion timeframes by March 31, 2025.

Recommendation #5
Document and implement a process to track and complete supply chain risk assessments for all third-party systems and service providers.

Management Response: The NCUA agrees with this recommendation. The NCUA is implementing a new solution that will allow for full coverage of all third-party vendors and will complete the risk assessments by December 31, 2025.

Recommendation #6
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.

Management Response: The NCUA agrees with this recommendation. The NCUA will implement an improved process for monitoring and managing this area by March 31, 2025.

Recommendation #7
Complete the 2024 backlog of overdue reinvestigations.

Management Response: The NCUA agrees with this recommendation. Reinvestigations, as required, will be completed by December 31, 2024.

Recommendation #8
Document and implement a process for notifying OHR [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.

Management Response: The NCUA agrees with this recommendation. NCUA will document and implement a process to notify OHR to add the initial role-based security training to the learning profile of new hires that are privileged users by December 31, 2024.

Recommendation #9
Complete implementation of the new alternate processing and storage site to a fully operational state.

Management Response: The NCUA agrees with this recommendation. While the NCUA will make substantial progress on this project by December 31, 2024, complete fail-over processing and storage services will be implemented by December 31, 2025.

Please contact Cybersecurity Advisor and Coordinator Todd Finkler if you have any questions.