



**NCUA**  
National Credit Union Administration

**OFFICE OF INSPECTOR  
GENERAL**

**NATIONAL CREDIT UNION ADMINISTRATION  
FEDERAL INFORMATION SECURITY MODERNIZATION  
ACT OF 2014 AUDIT - FISCAL YEAR 2023**

**Report #OIG-23-08  
September 14, 2023**





---

## National Credit Union Administration

---

### Office of Inspector General

SENT BY EMAIL

**TO:** Distribution List

**FROM:** Inspector General James W. Hagen *James W Hagen*

**SUBJECT:** National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2023

**DATE:** September 14, 2023

Attached is the Office of the Inspector General's FY 2023 independent evaluation of the effectiveness of the National Credit Union Administration's (NCUA) information security program and practices.<sup>1</sup>

The OIG engaged CliftonLarsonAllen LLP (CLA) to perform this evaluation.<sup>2</sup> 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 CLA's performance under this contract.

This report summarizes the results of CLA's independent evaluation and contains two 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 CLA 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.

---

<sup>1</sup> 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.

<sup>2</sup> CLA is an independent certified public accounting and consulting firm.

Distribution List:

Chairman Todd M. Harper  
Board Vice Chairman Kyle S. Hauptman  
Board Member Rodney E. Hood  
Executive Director Larry Fazio  
General Counsel Frank Kressman  
Deputy Executive Director Rendell Jones  
Chief of Staff Catherine Galicia  
OEAC Director Elizabeth Eurgubian  
Chief Information Officer Robert 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  
Senior Agency Information Security/Risk Officer David Tillman  
Cybersecurity Advisor and Coordinator Todd Finkler  
Senior Agency Official for Privacy Linda Dent

Attachment

**National Credit Union Administration**  
**Federal Information Security Modernization Act of 2014 Audit**  
**Fiscal Year 2023**  
**Final Report**





Inspector General  
National Credit Union Administration

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the National Credit Union Administration's (NCUA) information security program and practices for fiscal year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA or the Act). FISMA requires agencies to develop, implement, and document an agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and report the results to the Office of Management and Budget (OMB).

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 based on responding to the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2023 IG FISMA Reporting Metrics).

For this year's review, OMB required IGs to assess 20 Core and 20 FY 2023 supplemental IG FISMA Reporting Metrics in the following five security function areas to assess the maturity level and the effectiveness of their agencies' information security program: Identify, Protect, Detect, Respond, and Recover.<sup>1</sup> The maturity levels ranging from lowest to highest are: Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. According to the FY 2023 IG FISMA Reporting Metrics, Managed and Measurable and Optimized are considered effective maturity levels.

The audit included an assessment of NCUA's information security program and practices consistent with FISMA and reporting instructions issued by OMB. The scope also included assessing selected controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to the FY 2023 IG FISMA Reporting Metrics, for a sample of 4 of 58 NCUA internal and external information systems in NCUA's inventory of information systems as of February 2023.

Audit fieldwork covered NCUA's headquarters located in Alexandria, VA, from March 17, 2023, to July 6, 2023, assessing the period from October 1, 2022, through July 6, 2023.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

---

<sup>1</sup> The function areas are further broken down into nine domains.


We concluded that NCUA implemented an effective information security program by achieving an overall *Managed and Measurable* maturity level, complied with FISMA, and substantially complied with Agency information security and privacy, practices, policies and procedures. Although NCUA implemented an effective information security program, its implementation of a subset of selected controls was not fully effective. Specifically, we noted four new weaknesses under the configuration management and identity and access management domains of the FY 2023 IG FISMA Reporting Metrics. As a result, we made two new recommendations to assist NCUA in strengthening its information security program. In addition, twelve prior FISMA recommendations remain open.

Our work did not include an assessment of the sufficiency of internal control over financial reporting or other matters not specifically outlined in the enclosed report. CLA cautions that projecting the results of our performance audit to future periods is subject to the risks that conditions may materially change from their current status. The information included in this report was obtained from NCUA on or before September 13, 2023. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 13, 2023.

The purpose of this audit report is to report on our assessment of the NCUA's compliance with FISMA and is not suitable for any other purpose.

Additional information on our findings and recommendations are included in the accompanying report. We provided this report to the NCUA Office of Inspector General.

**CliftonLarsonAllen LLP**

A handwritten signature in cursive script that reads "CliftonLarsonAllen LLP".

Arlington, Virginia  
September 13, 2023

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**TABLE OF CONTENTS**

**Executive Summary** ..... 1

**FISMA Audit Findings** ..... 6

**Security Function: Protect**.....6

        1. NCUA Did Not Consistently Implement an Automated Process to Disable Inactive Network User Accounts in Accordance with NCUA Policy ..... 6

        2. NCUA Needs to Strengthen its Vulnerability Management Program ..... 7

        3. NCUA Needs to Require Multifactor Authentication (MFA) to the NCUA Network for All Non-Privileged Users ..... 9

        4. NCUA Needs to Ensure Rules of Behavior Are Consistently Completed Timely for New Contractors ..... 10

**Appendix I – Background** ..... 11

**Appendix II – Objective, Scope, and Methodology**..... 14

**Appendix III – Status of Prior Year Recommendations**..... 17

**Appendix IV – Management Comments** ..... 20

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

# **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's (NCUA) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit for Fiscal Year (FY) 2023 in accordance with the Federal Information Security Modernization Act of 2014 in support of the FISMA requirement for an annual 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 based on responding to the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2023 IG FISMA Reporting Metrics).

The FY 2023 IG FISMA Reporting Metrics requires us to assess the maturity of five functional areas in the Agency's information security programs and practices. For this year's review, IGs were required to assess 20 Core<sup>2</sup> and 20 Supplemental<sup>3</sup> IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover – to determine the effectiveness of their agencies' 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 I for additional information on the FY 2023 IG FISMA Reporting Metrics and FISMA reporting requirements.

For this audit, we reviewed selected controls<sup>4</sup> outlined in NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, mapped to

---

<sup>2</sup> 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.

<sup>3</sup> Supplemental Metrics are assessed at least once every two years and represent important activities conducted by security programs and contribute to the overall evaluation and determination of security program effectiveness.

<sup>4</sup> The controls were tested to the extent necessary to determine whether NCUA implemented the processes specifically addressed in the IG FISMA Reporting Metrics. In addition, not all controls were tested for all four sampled information systems since several controls were inherited from NCUA's general support system and certain controls were not applicable for external systems.



**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

the FY 2023 IG FISMA Reporting Metrics for a sample of 4 of 58 NCUA internal and external information systems<sup>5</sup> in NCUA’s FISMA inventory as of February 23, 2023.

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

**Audit Results**

We concluded that NCUA implemented an effective information security program by achieving an overall Level 4 - *Managed and Measurable* maturity level, complied with FISMA, and substantially complied with agency information security and privacy policies and procedures. **Table 1** below summarizes the overall maturity levels for each security function and domain in the FY 2023 IG FISMA Reporting Metrics. Four Cybersecurity Framework Function areas were determined to be at the *Managed and Measurable* (Level 4) maturity level and the fifth Cybersecurity Framework Function area was determined to be at the *Consistently Implemented* (Level 3) maturity level.

**Table 1: Assessed Maturity Levels for FY 2023 IG FISMA Reporting Metrics**

<b>Security Functions</b>	<b>Assessed FY 2023 Maturity Level by Function</b>	<b>Metric Domains</b>	<b>Assessed FY 2023 Maturity Level by Domain</b>
<b>Identify</b>	Managed and Measurable (Level 4)	<b>Risk Management</b>	Optimized (Level 5)
		<b>Supply Chain Risk Management</b>	Ad-Hoc (Level 1)
<b>Protect</b>	Consistently Implemented (Level 3)	<b>Configuration Management</b>	Consistently Implemented (Level 3)
		<b>Identity and Access Management</b>	Consistently Implemented (Level 3)
		<b>Data Protection and Privacy</b>	Consistently Implemented (Level 3)
		<b>Security Training</b>	Managed and Measurable (Level 4)
<b>Detect</b>	Managed and Measurable (Level 4)	<b>Information Security Continuous Monitoring</b>	Managed and Measurable (Level 4)
<b>Respond</b>	Managed and Measurable (Level 4)	<b>Incident Response</b>	Managed and Measurable (Level 4)
<b>Recover</b>	Managed and Measurable (Level 4)	<b>Contingency Planning</b>	Managed and Measurable (Level 4)
<b>Overall</b>	<b>Managed and Measurable (Level 4) Effective</b>		

In accordance with the FY 2023 IG FISMA Reporting Metrics guidance,<sup>6</sup> we focused on the calculated average of the Core IG FISMA Reporting Metrics. Additionally, we considered other

<sup>5</sup> 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.

<sup>6</sup> The FY 2023 IG FISMA Reporting Metrics provided the agency IG 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

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

data points, such as the calculated average of the Supplemental IG FISMA Reporting Metrics and FY 2023 testing results to come to this risk-based conclusion. We noted improvement since last year for the two modified repeat findings. In addition, the new weaknesses we identified during this year’s audit, in combination with the status of the prior FISMA recommendations, did not have a significant enough impact on the NCUA’s overall information security program for us to consider it ineffective. As a result, the NCUA’s overall maturity was assessed as *Managed and Measurable (Effective)*.<sup>7</sup>

In addition, NCUA took corrective action to close 2 of the 14 prior FISMA open recommendations from the FY 2018,<sup>8</sup> FY 2019,<sup>9</sup> FY 2021,<sup>10</sup> and FY 2022<sup>11</sup> FISMA audits. Refer to **Appendix III** for the status of prior year recommendations. Implementing more of these recommendations will help NCUA continue to strengthen its information security program.

Although we concluded that NCUA implemented an effective information security program overall, its implementation of a subset of selected controls was not fully effective. We noted four new weaknesses that fell in the configuration management and identity and access management domains of the FY 2023 IG FISMA Reporting Metrics (see Findings 1 through 4 in **Table 2**). As a result, we made two new recommendations to assist NCUA in strengthening its information security program. **Table 2** also includes weaknesses where NCUA has 12 prior year recommendations that remain open. These control weaknesses affect the NCUA’s ability to preserve the confidentiality, integrity, and availability of their information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

**Table 2: Weaknesses Noted in FY 2023 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2023 IG FISMA Reporting Metrics**

Cybersecurity Framework Security Function	FY 2023 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	Risk Management	<p>The NCUA needs to ensure external system interconnection agreements are kept up to date. (<b>Open prior year recommendation</b>)<sup>12</sup></p> <p>The NCUA needs to properly manage unauthorized software on the agency’s</p>

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 lower level than level 4.

<sup>7</sup> The FY 2023 IG FISMA Reporting Metrics were provided as a separate deliverable. The FY 2023 IG FISMA Reporting Metrics deliverable included calculated averages for the FY 2023 Core IG FISMA Reporting Metrics and Supplemental IG FISMA Reporting Metrics.

<sup>8</sup> *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).

<sup>9</sup> *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2019* (Report No. OIG-19-10, December 12, 2019).

<sup>10</sup> *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2021* (OIG Report No. OIG-21-09 November 22, 2021).

<sup>11</sup> *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (Report No. OIG-22-07, October 26, 2022).

<sup>12</sup> Recommendation 1, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (Report No. OIG-22-07, October 26, 2022).

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

Cybersecurity Framework Security Function	FY 2023 IG FISMA Reporting Metrics Domain	Weaknesses Noted
		network. ( <b>Open prior year recommendation</b> ) <sup>13</sup>
	<b>Supply Chain Risk Management</b>	The NCUA needs to enhance its Supply Chain Risk Management strategy, policies, and procedures. ( <b>Open prior year recommendation</b> ) <sup>14</sup>
<b>Protect</b>	<b>Configuration Management</b>	The NCUA needs to strengthen its vulnerability management program including remediating vulnerabilities in accordance with agency policy and migrating unsupported software to supported platforms. ( <b>Finding 2 (Modified Repeat) &amp; 4 open prior year recommendations</b> ) <sup>15</sup>
		The NCUA needs to implement standard baseline configuration settings in accordance with NIST requirements and NCUA policy. ( <b>Open prior year recommendation</b> ) <sup>16</sup>
	<b>Identity and Access Management</b>	The NCUA did not consistently implement an automated process to disable inactive network user accounts in accordance with NCUA policy. ( <b>Finding 1</b> )
		The NCUA needs to require multifactor authentication to the NCUA network for all privileged and non-privileged users. ( <b>Finding 3 (Modified Repeat) &amp; open prior year recommendation</b> ) <sup>17</sup>
		The NCUA needs to document and implement a process to validate that all contractors acknowledge that they have read, understand, and agree to abide by the information system rules of behavior prior to granting information system access. ( <b>Finding 4</b> )

<sup>13</sup> Recommendation 10, *FY 2018 Independent Evaluation of the National Credit Union Administration's Compliance with the Federal Information Security Modernization Act of 2014* (OIG Report No. OIG-18-07, October 31, 2018).

<sup>14</sup> Recommendation 1, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2021* (OIG Report No. OIG-21-09 November 22, 2021).

<sup>15</sup> 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* (OIG Report No. OIG-18-07, October 31, 2018); and Recommendation 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).

<sup>16</sup> Recommendation 4, *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit*, (OIG Report No. OIG-19-10, December 12, 2019).

<sup>17</sup> Recommendation 2, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2021* (OIG Report No. OIG-21-09 November 22, 2021).

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

Cybersecurity Framework Security Function	FY 2023 IG FISMA Reporting Metrics Domain	Weaknesses Noted
		The NCUA needs to Implement a solution that resolves the privileged access management vulnerability. <b>(Open prior year recommendation)</b> <sup>18</sup>
	<b>Data Protection and Privacy</b>	The NCUA needs to implement media marking controls. <b>(2 open prior year recommendations)</b> <sup>19</sup>
	<b>Security Training</b>	None
<b>Detect</b>	<b>Information Security Continuous Monitoring</b>	None
<b>Respond</b>	<b>Incident Response</b>	The NCUA needs to employ file integrity monitoring tools. <b>(Open prior year recommendation)</b> <sup>20</sup>  The NCUA needs to strengthen its Security Information and Event Management tool audit logging collection, visibility, and retention processes. <b>(See recommendation from prior audit report)</b> <sup>21</sup>
<b>Recover</b>	<b>Contingency Planning</b>	None

The following section provides a detailed discussion of the audit findings. Appendix I provides background information on NCUA and the FISMA legislation, Appendix II describes the audit objective, scope, and methodology, Appendix III provides the status of prior year recommendations, and Appendix IV includes management’s comments.

<sup>18</sup> 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).

<sup>19</sup> Recommendations 5 and 6, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2021* (OIG Report No. OIG-21-09 November 22, 2021).

<sup>20</sup> Recommendation 7, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2021* (OIG Report No. OIG-21-09 November 22, 2021).

<sup>21</sup> Recommendations 2, 3 and 4, *National Credit Union Administration Cybersecurity Audit* (OIG Report No. OIG 23-05, May 2, 2023).

# FISMA Audit Findings

## Security Function: Protect

---

### 1. NCUA Did Not Consistently Implement an Automated Process to Disable Inactive Network User Accounts in Accordance with NCUA Policy.

**FY 2023 Metrics Domain:** *Identity and Access Management*

NCUA did not consistently implement an automated process to disable inactive network user accounts after 30 days of inactivity in accordance with NCUA policy. As a result, out of the total population of 1,484 network user accounts, NCUA did not disable three privileged accounts and eight non-privileged accounts that had been inactive for 30 days or more.

The *NCUA Information Security Procedural Manual* requires automatically disabling of inactive accounts after 30 days of inactivity.

NIST Special Publication (SP) 800-53, Revision 5, security control Access Control (AC)-2, Account Management requires organizations to implement the following regarding inactive accounts:

- Create, enable, modify, disable, and remove information system accounts in accordance with [Assignment: organization-defined procedures or conditions];
- Support the management of system accounts using [Assignment: organization-defined automated mechanisms].
- Disable accounts within [Assignment: organization-defined time period] when the accounts have been inactive for [Assignment: organization-defined time-period].

Management specified that the automated script that runs to disable accounts after 30 days of inactivity was not updated to include a new domain controller<sup>22</sup> that had replaced a decommissioned domain controller on February 14, 2023. In response to the auditors notifying management of this issue during the audit, management initiated the automated script on the new domain controller on May 26, 2023.

Malicious actors can use dormant accounts to gain unauthorized access to information systems. If dormant accounts are not detected and deactivated, an unauthorized user's activity may go unnoticed. By ensuring inactive accounts are disabled in accordance with NCUA policy, NCUA can reduce the risk of unauthorized access, decreasing the likelihood of unauthorized modification, loss, and disclosure of sensitive NCUA information, and reduce the risk of disrupting mission critical agency systems.

---

<sup>22</sup> A domain controller authenticates users within a Microsoft Windows server domain.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

To assist NCUA with automatically disabling inactive network user accounts, we recommend that NCUA management:

**FY 2023 Recommendation 1:** 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.

**Agency Response:**

The NCUA agrees with the recommendation. This finding has been remediated. The NCUA has updated our related change management procedures to confirm that server policies and/or related automated scripts are configured and running as desired after a change is made to the server environment.

**OIG Response:**

We concur with management's specified action and will validate completion during the FY 2024 FISMA audit.

**2. NCUA Needs to Strengthen its Vulnerability Management Program.**

**FY 2023 Metrics Domain:** *Configuration Management*

We conducted independent vulnerability scans utilizing Nessus. Using vulnerability data from the Common Vulnerability Scoring System (CVSS<sup>23</sup>) used by Nessus, we identified unpatched software, unsupported software, and improper configuration settings that exposed the NCUA Headquarters network to critical<sup>24</sup> and high<sup>25</sup> severity vulnerabilities. In addition, NCUA did not resolve critical and high-risk vulnerabilities within 30 days of occurrence, as required by its internal operating policies. Furthermore, NCUA did not timely remediate older vulnerabilities that were publicly known before 2023.

The credential scans of 304 hosts identified unique critical and high-risk vulnerabilities related to patch management, configuration management, and unsupported software falling outside of NCUA's remediation timeframe.<sup>26</sup> Some of these vulnerabilities included:

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

I [Redacted]

---

<sup>23</sup> The Common Vulnerability Scoring System (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.

<sup>24</sup> 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.

<sup>25</sup> High vulnerabilities possess a CVSS rating of 7 to 9.9.

<sup>26</sup> (b) (7)(E) [Redacted]

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

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

- Critical or High Vulnerabilities (with CVSS score of 7 to 10) must be corrected within 30 days, after which a POA&M must be established.
- Moderate (Medium) Vulnerabilities (with CVSS score of 4 to 6.9) must be corrected within 60 days after which a POA&M must be established.
- Low Vulnerabilities (with CVSS score of 0 to 3.9) must be corrected after high and moderate vulnerabilities are corrected as time permits. POA&Ms do not need to be established.

NIST SP 800-53, Revision 5, control System and Information Integrity (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.

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

- 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.

We conducted independent 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.<sup>27</sup> We conducted additional scans in 2020, 2021, and 2022 with similar results. In 2022, we made additional recommendations related to developing a staffing plan to allocate appropriate and sufficient resources to improve Office of the Chief Information Officers' (OCIO) ability to perform remediation of persistent vulnerabilities and developing plan to reduce the wide variety of differing technologies requiring support and vulnerability remediation, as feasible.<sup>28</sup> Each of these prior recommendations remain open.

NCUA has been working to resolve the prior year recommendations related to vulnerability management. The overall number of un-remediated vulnerabilities identified during our scans has decreased significantly from the prior year; however, there are still outstanding vulnerabilities that require remediation. Although NCUA management has documented acceptance of risk with compensating controls for some of the vulnerabilities identified, there are still vulnerabilities present that are outside the defined patching timeframe.

---

<sup>27</sup> 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* (OIG Report No. OIG-18-07, October 31, 2018)

<sup>28</sup> Recommendations 2 and 3, *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2022* (OIG Report No. OIG-22-07, October 26, 2022).

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

By timely installing required patches, implementing secure configuration settings, and migrating to supported software, NCUA can mitigate the security weaknesses and limit the potential for attackers to compromise the confidentiality, integrity, and availability of sensitive credit union and employee data. This ultimately will improve the overall security posture of NCUA information systems.

No new recommendations will be made this year as management is working to address the prior year recommendations from the FY 2018 and FY 2022 reports.

### **3. NCUA Needs to Require Multifactor Authentication (MFA) to the NCUA Network for All Non-Privileged Users.**

#### **FY 2023 Metrics Domain: *Identity and Access Management***

We identified (b) (7)(E) total non-privileged network users did not use multifactor authentication.

Both NIST SP 800-53, Revision 5, control Identification and Authentication (IA)-2, IA (Organizational Users), Control Enhancement 2 and the *NCUA Information Security Procedural Manual* require the implementation of multi-factor authentication for access to non-privileged accounts.

Management stated that since last year, NCUA distributed Personal Identity Verification (PIV) cards in a timelier manner than the previous two years. Although the number of users who do not have a PIV card or Duo multifactor authentication has decreased since last year from 241 users, 70 users still do not use multifactor authentication to access NCUA's network. In response to the 2021 FISMA audit recommendation to address this issue,<sup>29</sup> management stated the agency would develop and implement a plan by July 31, 2022, to deploy multifactor authentication for network users who do not have a PIV card. Management stated that the agency plans to implement YubiKey's as an additional multifactor authentication solution this calendar year.

Multifactor authentication employs an additional layer of security when users log into NCUA's network by requiring at least two methods for verifying a user's identity. By requiring multifactor authentication for all NCUA network user accounts, the risk of unapproved access leading to unauthorized modification, loss, and disclosure of sensitive NCUA information or personally identifiable information is decreased.

Since the FY 2021 FISMA recommendation to document and implement a plan to deploy multifactor authentication for users without a PIV card is still open, we are not making any new recommendations regarding multifactor authentication for non-privileged users.

---

<sup>29</sup> Ibid 18.



**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

#### **4. NCUA Needs to Ensure Rules of Behavior Are Consistently Completed Timely for New Contractors.**

**FY 2023 Metrics Domain:** *Identity and Access Management*

Two from a sample of five new contractors hired since October 1, 2022, did not complete the NCUA Rules of Behavior prior to gaining network access in accordance with NIST requirements and NCUA policy. The sampled contractors acknowledged the Rules of Behavior between 67 and 166 days after the dates they onboarded at NCUA and received network access.

Both NIST SP 800-53, Revision 5, control Planning (PL)-4, Rules of Behavior, and the NCUA *Information Security Procedural Manual* require that individuals needing system access acknowledge that they have read, understand, and agree to abide by the rules of behavior before authorizing access to information and information systems.

Management specified that the NCUA uses a SharePoint workflow process for onboarding new contractors and employees. In the case of the two sampled individuals, the NCUA was in the process of migrating to SharePoint Online, which caused a disruption in the workflow. The Learning and Managing Performance (LAMP) system is configured to automatically create training accounts and assign the initial security awareness training that includes acknowledgement of the NCUA Rules of Behavior from the SharePoint workflow process. Because of this transition related to the SharePoint migration, the data feed to LAMP did not occur until later. Management further indicated that the SharePoint migration has been completed and the automation is now working as intended however evidence was not provided to us for validation.

Rules of Behavior establish responsibilities and expected actions for users of NCUA information systems specifying what users are permitted and/or not permitted to do when accessing those systems. By ensuring all users acknowledge that they have read, understand, and agree to abide by the rules of behavior before gaining access to NCUA information and information systems, NCUA can reduce the risk of system users not knowing or understanding their information security responsibilities and hold users accountable to follow the specified requirements.

To assist NCUA with consistently completing rules of behavior for new contractors, we recommend that NCUA management:

***FY 2023 Recommendation 2:*** 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.

**Agency Response:**

The NCUA agrees with the recommendation. The NCUA is in the process of updating the automated onboarding workflow and process to confirm the NCUA Rules of Behavior are completed timely upon onboarding. The estimated completion date is December 31, 2023.

**OIG Response:**

We concur with management's planned action.

# BACKGROUND

## National Credit Union Administration

Created by the U.S. Congress in 1970, the NCUA is an independent federal agency that insures deposits at federally insured credit unions, protects the members who own credit unions, and charters and regulates federal credit unions. The NCUA's operating fund contains the attributes of a revolving fund,<sup>30</sup> which is a permanent appropriation. The NCUA's mission is to "Provide, through regulation and supervision, a safe and sound credit union system, which promotes confidence in the national system of cooperative credit."

## FISMA Legislation

FISMA requires agencies to develop, document, and implement agency-wide programs to provide information security for the information and information systems that support their operations and assets and requires the agencies' IG to test the security of a representative subset of the agency's systems and assess the effectiveness of information security policies, procedures, and practices of the agency.

In addition, FISMA requires agencies to implement the following:

- Periodic risk assessments.
- Information security policies, procedures, standards, and guidelines.
- Delegation of authority to the Chief Information Officer (CIO) to ensure compliance with policy.
- Security awareness training programs.
- Periodic (annual and more frequent) testing and evaluation of the effectiveness of security policies, procedures, and practices.
- Processes to manage remedial actions for addressing deficiencies.
- Procedures for detecting, reporting, and responding to security incidents.
- Plans to ensure continuity of operations.
- Annual reporting on the adequacy and effectiveness of its information security program.

## ***FISMA Reporting Requirements***

OMB and the Department of Homeland Security (DHS) annually provide instructions to federal agencies and IGs for preparing FISMA reports. On December 2, 2022, OMB issued Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes key changes to the methodology for conducting

---

<sup>30</sup> A revolving fund amounts to "a permanent authorization for a program to be financed, in whole or in part, through the use of its collections to carry out future operations."

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix I**

FISMA audits; and the processes for federal agencies to report to OMB, and where applicable, DHS. Key changes to the methodology included:

- Selection of 20 Supplemental IG FISMA Reporting Metrics that must be evaluated during FY 2023, in addition to the 20 Core IG FISMA Reporting Metrics that must be evaluated annually.
- The remainder of standards and controls will be evaluated on a two-year cycle.
- In previous years, IGs have been directed to utilize a mode-based scoring approach to assess maturity levels. In FY 2023, ratings were focused on calculated averages, wherein the average of the metrics in a particular domain would be used by IGs to determine the effectiveness of individual function areas (Identify, Protect, Detect, Respond, and Recover). IGs were encouraged to focus on the calculated averages of the 20 Core IG FISMA Reporting Metrics, as these tie directly to Administration priorities and other high-risk areas. In addition, OMB M-23-03 indicated that IGs should use the calculated averages of the Supplemental IG FISMA Reporting Metrics and progress addressing outstanding prior year recommendations as data points to support their risk-based determination of overall program and function level effectiveness. The calculated averages can be found in the FY 2023 IG FISMA Reporting Metrics.

The FY 2023 IG FISMA Reporting Metrics provided the reporting requirements across key areas to be addressed in the independent assessment of agencies’ information security programs.

For this year’s review, IGs were to assess the 20 Core and 20 Supplemental IG FISMA Reporting Metrics in the five security function areas to assess the maturity level and effectiveness of their agency’s information security program. As highlighted in **Table 3**, 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 Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover.

**Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2023 IG FISMA Reporting Metrics Domains**

Cybersecurity	Domains in the FY 2023 IG FISMA Reporting Metrics
Identify	Risk Management, Supply Chain Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model in the FY 2023 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 4** 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*.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix I**

**Table 4: IG Evaluation Maturity Levels**

<b>Maturity Level</b>	<b>Maturity Level Description</b>
Level 1: Ad-hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy 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 strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

# 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 NCUA's information security program and practices based on responding to the *FY 2023-2024 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics* (FY 2023 IG FISMA Reporting Metrics).

## Scope

We conducted this performance audit in accordance with generally accepted government auditing standards. 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.

The scope of this performance audit was to assess NCUA's information security program consistent with FISMA and reporting instructions issued by OMB and DHS. The scope also included assessing selected controls outlined in NIST SP 800-53, Revision 5, mapped to the FY 2023 IG FISMA Reporting Metrics for a sample of 4 of 58 internal and external information systems<sup>31</sup> in NCUA's FISMA inventory as of February 23, 2023.

In addition, we performed an internal vulnerability assessment of NCUA's network and an assessment of the vulnerability management process for the Modern Examination and Risk Identification Tool (MERIT). The audit also included a follow up on prior audit recommendations<sup>32</sup> to determine whether NCUA made progress in implementing them. See Appendix III for the status of the prior recommendations.

For this year's review, IGs were to assess 20 Core and 20 Supplemental IG FISMA Reporting Metrics across five security function areas — Identify, Protect, Detect, Respond, and Recover — to determine the effectiveness of their agencies' information security program and the maturity level of each function area. The maturity levels range from lowest to highest — Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized.

Audit fieldwork covered NCUA's headquarters located in Alexandria, VA, from March 17, 2023, to July 6, 2023. It covered the period from October 1, 2022, through July 6, 2023.

The FY 2023 IG FISMA Reporting Metrics introduced a calculated average scoring model for FY 2023 and FY 2024 FISMA audits. As part of this approach, Core and Supplemental IG FISMA

---

<sup>31</sup> Ibid 5.

<sup>32</sup> Ibid 8, 9, 10, and 11.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix II**

Reporting Metrics were averaged independently to determine a domain's maturity calculation and provide data points for the assessed program and function effectiveness. 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, 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. It was 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 overall program and function level effectiveness.

We utilized the FY 2023 IG FISMA Reporting Metrics guidance<sup>33</sup> to form our conclusions for each Cybersecurity Framework domain, function, and the overall agency rating. Specifically, we focused on the calculated average of the Core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average of the Supplemental IG FISMA Reporting Metrics and FY 2023 testing results to come to this risk-based conclusion.

## **Methodology**

To determine if NCUA implemented an effective information security program, we conducted interviews with NCUA officials and contractors and reviewed legal and regulatory requirements stipulated in FISMA. In addition, we reviewed documents supporting the information security program. These documents included, but were not limited to, NCUA's (1) information security policies and procedures; (2) incident response policies and procedures; (3) access control procedures; (4) patch management procedures; (5) change control documentation; and (6) system generated account listings. Where appropriate, we compared documents, such as NCUA's information technology policies and procedures, to requirements stipulated in Executive Order (EO) 14028, relevant OMB memorandums, and NIST special publications. We also performed tests of system processes to determine the adequacy and effectiveness of those controls. Finally, we reviewed the status of FISMA audit recommendations from FY 2018,<sup>34</sup> FY 2019,<sup>35</sup> FY 2021,<sup>36</sup> and FY 2022.<sup>37</sup> See Appendix III for the status of prior year recommendations.

In assessing the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity (not the percentage of deficient items found compared to the total population available for review). In some cases, based on risk, significance, or criticality this resulted in selecting the entire population.

---

<sup>33</sup> The FY 2023 IG FISMA Reporting Metrics provided the agency IG 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 lower level than level 4.

<sup>34</sup> Ibid 8.

<sup>35</sup> Ibid 9.

<sup>36</sup> Ibid 10.

<sup>37</sup> Ibid 11.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix II**

However, in cases where the entire evaluation population was not selected, the results cannot be projected and if projected may be misleading.

To perform our audit of NCUA's information security program and practices, we followed a work plan based on, but not limited to, the following guidance:

- *Government Auditing Standards* (April 2021).
- Executive Order 14028, *Improving the Nation's Cybersecurity* (May 12, 2021).
- OMB Memorandum M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements* (December 2, 2022).
- OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021).
- OMB Memorandum M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices* (September 14, 2022).
- CISA's BOD 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities*.
- FY 2023 IG FISMA Reporting Metrics (February 10, 2023).
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for specification of security controls (December 10, 2020).
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, for the assessment of security control effectiveness.
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (November 11, 2011).
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations, A System Life Cycle Approach for Security and Privacy*, for the risk management framework controls (December 2018).
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework) (February 2014).
- NCUA policies and procedures.

We selected 4 information systems from the total population of 58 FISMA reportable systems for testing. The four systems were selected based on risk, date of last evaluation, criticality, and review of prior year audit findings. Specifically, the NCUA General Support System was selected based on risk since it is categorized as a moderate impact system<sup>38</sup> and supports NCUA applications that reside on the network. The Examination and Supervision System – Infrastructure Hosting (ESS-IH) was selected because it is the general support system for MERIT which replaced the Automated Integrated Regulatory Examination System (AIRES) in 2021 as the system of record for credit union exams. The Concur application is a cloud-based expense and travel management software used to monitor travel expenses. Okta is a cloud-based identity and access management software that helps secure user authentication and build identity controls applications, web services, and devices. We tested the four systems' selected security controls to support our responses to the FY 2023 IG FISMA Reporting Metrics.

---

<sup>38</sup> The selected systems were categorized as moderate impact based on NIST Federal Information Processing Standards Publication 199 *Standards for Security Categorization of Federal Information and Information System*.

# STATUS OF PRIOR YEAR RECOMMENDATIONS

The table below summarizes the status of our follow up related to the prior recommendations reported for the FY 2018,<sup>39</sup> 2019,<sup>40</sup> 2021,<sup>41</sup> and 2022<sup>42</sup> FISMA audits. During FY 2023, the NCUA implemented corrective actions to close two prior year recommendations.

Audit Year and Recommendation	Status Determined by NCUA	Auditor Position on Status of Recommendation
<b>2018-6:</b> The Office of Continuity and Security Management complete its employee background re-investigations.	Closed	Closed
<b>2018-8:</b> The Office of the Chief Information Officer enforce the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.	Open	Open See finding 2
<b>2018-9:</b> The Office of the Chief Information Officer implement a process to detect and migrate unsupported software to supported platforms before support for the software ends.	Open	Open See finding 2
<b>2018-10:</b> The Office of the Chief Information Officer implement a process to identify authorized software in its environment and remove any unauthorized software.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions were scheduled for completion by November 30, 2020. However, according to NCUA management, corrective action has not been completed.
<b>2019-4:</b> The NCUA management ensures the Agency implements, tests, and monitors standard baseline configurations for all platforms in the NCUA information technology environment in compliance with	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not

<sup>39</sup> Ibid 8.

<sup>40</sup> Ibid 9.

<sup>41</sup> Ibid 10.

<sup>42</sup> Ibid 11.



**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix III**

Audit Year and Recommendation	Status Determined by NCUA	Auditor Position on Status of Recommendation
established NCUA security standards. This includes documenting approved deviations from the configuration baselines with business justifications.		scheduled for completion until December 31, 2024.
<b>2021-1:</b> Review the SCRM NIST guidance and update the SCRM plan, policies, and procedures to fully address supply chain risk management controls and practices.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions were scheduled for completion by December 2022. However according to NCUA management, corrective action has not been completed.
<b>2021-2:</b> 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.	Open	Open  See finding 3
<b>2021-5:</b> Complete and issue policies to implement the CUI program.	Closed	Closed
<b>2021-6:</b> Upon issuance of the CUI policies, design and implement media marking to designate protection standards for safeguarding and/or disseminating agency information.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions were scheduled for completion by December 2022. However according to NCUA management, corrective action has not been completed.
<b>2021-7:</b> Select and implement a tool for file integrity monitoring.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until September 2023.
<b>2022-1:</b> Enforce the process to validate that expired MOUs and those expiring are prioritized for review, update, and	Open	Open

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix III**

Audit Year and Recommendation Number	Status Determined by NCUA	Auditor Position on Status of Recommendation
renewal in accordance with NCUA policy.		Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until December 29, 2023.
<b>2022-2:</b> 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.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until August 31, 2023. <sup>43</sup>
<b>2022-3:</b> 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.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until August 31, 2023. <sup>44</sup>
<b>2022-4:</b> Implement a solution that resolves the privileged access management vulnerability	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until January 31, 2024.

<sup>43</sup> Audit fieldwork ended on July 6, 2023; therefore, corrective action will be validated during the FY 2024 FISMA audit.

<sup>44</sup> Ibid 43.

# MANAGEMENT COMMENTS



National Credit Union Administration  
Office of the Executive Director

SENT BY EMAIL

**TO:** Inspector General James Hagen  
**FROM:** Executive Director Larry Fazio Digitally signed by LARRY FAZIO  
FAZIO  
Date: 2023.09.01 12:54:18  
+0400  
**SUBJ:** Draft Report for Federal Information Security Modernization Act of 2014  
Audit Fiscal Year 2023  
**DATE:** September 01, 2023

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 2023*. The draft report concludes that 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 NCUA’s continuing commitment to strong information security.

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

## **Recommendation #1**

Document 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.

**Management Response:** The NCUA agrees with the recommendation. This finding has been remediated. The NCUA has updated our related change management procedures to confirm that server policies and/or related automated scripts are configured and running as desired after a change is made to the server environment.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2023 FISMA AUDIT**

**Appendix IV**

**Recommendation #2**

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.

Management Response: The NCUA agrees with the recommendation. The NCUA is in the process of updating the automated onboarding workflow and process to confirm the NCUA Rules of Behavior are completed timely upon onboarding. The estimated completion date is December 31, 2023.

**Status of Prior Year Recommendations**

Please see the attached update to the status of the open prior year recommendations.

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

Attachment

cc: NCUA Board Members  
OEAC  
Deputy Executive Director Rendell Jones Cybersecurity  
Advisor and Coordinator Todd Finkler