



**NCUA**  
National Credit Union Administration

**OFFICE OF INSPECTOR  
GENERAL**

**NATIONAL CREDIT UNION ADMINISTRATION  
FEDERAL INFORMATION SECURITY MODERNIZATION  
ACT OF 2014 AUDIT – FISCAL YEAR 2022**

**Report #OIG-22-07  
October 26, 2022**



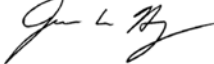


---

**Office of Inspector General**

SENT BY EMAIL

**TO:** Distribution List

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

**SUBJ:** National Credit Union Administration Federal Information Security  
Modernization Act of 2014 Audit—Fiscal Year 2022

**DATE:** October 26, 2022

Attached is the Office of the Inspector General's FY 2022 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 four 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 planned 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 Deputy Director Samuel Schumach  
Chief Information Officer Robert Foster  
Chief Financial Officer Eugene Schied  
Regional Director and AMAC President Keith Morton  
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  
Senior Agency Official for Privacy Linda Dent

Attachment

**National Credit Union Administration**  
**Federal Information Security Modernization Act of 2014 Audit**  
**Fiscal Year 2022**  
**Final Report**



CPAs | CONSULTANTS | WEALTH ADVISORS

[CLAconnect.com](https://CLAconnect.com)



CliftonLarsonAllen LLP  
901 North Glebe Road, Suite 200  
Arlington, VA 22203

phone 571-227-9500 fax 571-227-9552  
CLAconnect.com

October 25, 2022

James Hagen  
Inspector General  
National Credit Union Administration  
1775 Duke Street  
Alexandria, VA 22314

Dear Mr. Hagen:

CliftonLarsonAllen LLP (CLA) is pleased to present our report on the results of our performance audit of the National Credit Union Administration's (NCUA) information security program and practices in accordance with the Federal Information Security Modernization Act of 2014 for the fiscal year 2022.

We appreciate the assistance we received from the NCUA. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

Sarah Mirzakhani, CISA  
Principal



Inspector General  
National Credit Union Administration

CliftonLarsonAllen LLP (CLA) conducted a performance audit of the National Credit Union Administration's (NCUA or Agency) information security program and practices for fiscal year (FY) 2022 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 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 objectives of this performance audit were to (1) assess the NCUA's compliance with FISMA and agency information security and privacy policies and procedures; and (2) respond to the OMB Office of the Federal Chief Information Officer *FY 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* (FY 2022 Core Metrics).

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

For this year's review, OMB required Inspectors General to assess 20 Core Metrics in the following five security function areas to determine the effectiveness of their agencies' information security program and the maturity level of each area: Identify, Protect, Detect, Respond, and Recover. The maturity levels ranging from lowest to highest are Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized. The functions areas are further broken down into nine domains. To be considered effective, an agency's information security program must be rated Level 4 - *Managed and Measurable* overall.

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 security controls outlined in National Institute of Standards and Technology Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of 4 of 47 NCUA internal and external information systems in NCUA's inventory of information systems as of February 2022.

Audit fieldwork covered NCUA's headquarters located in Alexandria, VA, from March 30, 2022, to September 14, 2022, assessing the period from October 1, 2021, through September 30, 2022.

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. 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 that fell in the risk management, identity and access management, and configuration management domains of the FY 2022 Core Metrics. As a result, we are making four new recommendations to assist NCUA in

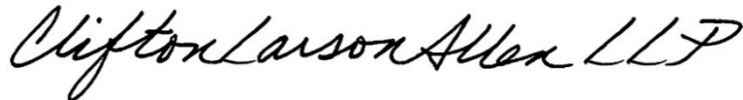
strengthening its information security program. In addition, ten prior FISMA recommendations remain open.

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 October 25, 2022. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to October 25, 2022.

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 OIG.

**CliftonLarsonAllen LLP**

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style.

Arlington, Virginia  
October 25, 2022

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**TABLE OF CONTENTS**

<b>Executive Summary .....</b>	<b>1</b>
<b>FISMA Audit Findings .....</b>	<b>5</b>
<b>Security Function: Identify .....</b>	<b>5</b>
1. The NCUA Needs to Ensure External System Interconnection Agreements are Kept Up to Date .....	5
<b>Security Function: Protect .....</b>	<b>7</b>
2. The NCUA Needs to Strengthen its Vulnerability Management Program .....	7
3. The NCUA Needs to Require Multifactor Authentication to the NCUA Network for all Privileged and Non-Privileged Users .....	9
4. The NCUA Did Not Automatically Disable Inactive Rainy Day SmartPayables User Accounts in Accordance with NCUA Policy .....	10
<b>Appendix I – Background .....</b>	<b>12</b>
<b>Appendix II – Objective, Scope, and Methodology .....</b>	<b>14</b>
<b>Appendix III – Status of Prior Year Recommendations .....</b>	<b>17</b>
<b>Appendix IV – Management Comments .....</b>	<b>20</b>



**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

# **EXECUTIVE SUMMARY**

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) 2022 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA or the Act) in support of the FISMA requirement for an annual evaluation of the NCUA's information security program and practices.

The objectives of this performance audit were to (1) assess the NCUA's compliance with FISMA and agency information security and privacy policies and procedures; and (2) respond to the Office of Management and Budget (OMB) Office of the Federal Chief Information Officer *FY 2022 Core Inspector General Metrics Implementation Analysis and Guidelines* (FY 2022 Core Metrics).

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. OMB and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow for implementing information security and privacy programs.

OMB and the Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 6, 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. According to that memorandum, each year the IGs are required to complete IG FISMA reporting metrics<sup>1</sup> to independently assess their agencies' information security program. OMB selected a core group of 20 metrics, representing a combination of Administration priorities and other highly valuable controls, that must be evaluated annually. The remainder of the standards and controls will be evaluated in metrics on a two-year cycle. In addition, OMB shifted the due date of the IG FISMA Reporting metrics from October to July to better align with the release of the President's budget.<sup>2</sup>

For FY 2022, OMB required IGs to assess the 20 Core Metrics in the five security function areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1: Identify, Protect, Detect, Respond, and Recover, to assess the maturity level and effectiveness of their agencies' information security program. 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*.

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 security controls outlined in NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for a sample of 4 of

---

<sup>1</sup> We submitted our responses to the FY 2022 IG FISMA reporting metrics to the NCUA OIG as a separate deliverable under the contract for this audit.

<sup>2</sup> OMB M-22-05 *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*, December 6, 2021.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

47 NCUA internal and external information systems in NCUA's inventory of information systems as of February 2022. We also completed follow-up on prior open FISMA recommendations.

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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

## **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 2022 Core Metrics.<sup>3</sup> Two Cybersecurity Framework Function areas were determined to be at the *Optimized* (Level 5) maturity level and the other three Cybersecurity Framework Function areas were determined to be at the *Managed and Measurable* (Level 4) maturity level.

**Table 1: Maturity Levels for FY 2022 Core Metrics**

<b>Security Function</b>	<b>Maturity Level by Function</b>	<b>FY 2022 Core Metrics Domains</b>	<b>Maturity Level by Domain</b>
<b>Identify</b>	Optimized (Level 5)	<b>Risk Management</b>	Optimized (Level 5)
		<b>Supply Chain Risk Management</b>	Ad-Hoc (Level 1)
<b>Protect</b>	Managed and Measurable (Level 4)	<b>Configuration Management</b>	Defined (Level 2)
		<b>Identity and Access Management</b>	Defined (Level 2)
		<b>Data Protection and Privacy</b>	Managed and Measurable (Level 4)
		<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>	Optimized (Level 5)	<b>Incident Response</b>	Optimized (Level 5)
<b>Recover</b>	Managed and Measurable (Level 4)	<b>Contingency Planning</b>	Managed and Measurable (Level 4)
<b>Overall Rating</b>	<b>Managed and Measurable (Level 4) Effective</b>		

<sup>3</sup> In accordance with the FY 2022 IG FISMA Reporting Metrics, ratings throughout the nine domains were determined by a simple majority, where the most frequent level across the metrics served as the domain rating. Agencies were rated at the higher level in instances when two or more levels were the most frequently rated. The domain ratings inform the overall function ratings, and the five function ratings inform the overall agency rating.

## NATIONAL CREDIT UNION ADMINISTRATION FY 2022 FISMA EVALUATION

In addition, NCUA took corrective action to close 2 of the 12 prior FISMA open recommendations from the FY 2018,<sup>4</sup> FY 2019,<sup>5</sup> and FY 2021<sup>6</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 risk management, identity and access management, and configuration management domains of the FY 2022 Core Metrics (see Findings 1 through 4 in Table 2) and have made four new recommendations to assist NCUA in strengthening its information security program. **Table 2** also includes weaknesses where NCUA has ten prior year recommendations that remain open. These control weaknesses affect the NCUA's ability to preserve the confidentiality, integrity, and availability of the Agency's information and information systems, potentially exposing them to unauthorized access, use, disclosure, disruption, modification, or destruction.

**Table 2: Weaknesses Noted in FY 2022 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2022 Core Metrics**

Cybersecurity Framework Security Function	FY 2022 Core Metrics Domain	Weaknesses Noted
Identify	Risk Management	The NCUA needs to ensure external system interconnection agreements are kept up to date. <b>(Finding 1)</b>  The NCUA needs to properly manage unauthorized software on the agency's network. <b>(Open prior year recommendation)</b> <sup>7</sup>
	Supply Chain Risk Management	The NCUA needs to enhance its Supply Chain Risk Management strategy, policies, and procedures. <b>(Open prior year recommendation)</b> <sup>8</sup>
Protect	Configuration Management	The NCUA needs to strengthen its vulnerability management program including remediating vulnerabilities in accordance with agency policy and migrating unsupported software to supported

<sup>4</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>5</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>6</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>7</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>8</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).

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

<b>Cybersecurity Framework Security Function</b>	<b>FY 2022 Core Metrics Domain</b>	<b>Weaknesses Noted</b>
		platforms. <b>(Finding 2 (Repeat) &amp; 2 Open prior year recommendations)</b> <sup>9</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>10</sup>
	<b>Identity and Access Management</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>11</sup>
		The NCUA did not automatically disable inactive rainy day SmartPayables user accounts in accordance with NCUA policy. <b>(Finding 4)</b>
		The NCUA needs to complete background re-investigations. <b>(Open prior year recommendation)</b> <sup>12</sup>
	<b>Data Protection and Privacy</b>	The NCUA needs to implement media marking controls. <b>(2 Open prior year recommendations)</b> <sup>13</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>14</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 includes the status of prior year recommendations, and Appendix IV includes management's comments.

<sup>9</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>10</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>11</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).

<sup>12</sup> Recommendation 6, *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>13</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>14</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).

# FISMA Audit Findings

## Security Function: Identify

---

### 1. The NCUA Needs to Ensure External System Interconnection Agreements are Kept Up to Date.

#### **FY 2022 Core Metrics Domain:** *Risk Management*

The Memorandum of Understanding (MOU) between NCUA and the Office of Personnel Management (OPM) Electronic Official Personnel Folder (eOPF) system expired in June 2021 and was not renewed.

Management stated that the eOPF MOU expired because the Information System Security Officers (ISSOs) did not have the resources to review and monitor the interconnection security agreements for all the NCUA systems/services. Therefore, the ISSOs focused on newer systems and services and the agreement for eOPF, an older external service, was not monitored.

NIST SP 800-53, Revision 5, security control CA-3, Information Exchange requires NCUA to approve and manage the exchange of information between agency systems and external systems using an interconnection security agreement or memorandum of understanding, and to review and update the agreements at an organization defined frequency.

The *NCUA Information Security Procedural Manual* requires the review and update of interconnection security agreements at least quarterly.

In addition, the *NCUA Assessment and Authorization (A&A) Standard Operating Procedures*, version 3.2 requires ISSOs to be aware of the status and the expiration of the applicable external system interconnection agreements, and initiate action early enough to avoid expiration of the agreements.

With an up-to-date MOU, NCUA is guaranteed that the responsibilities of all parties for establishing, operating, and securing the interconnection are documented, understood, current, and agreed to. The MOU serves to help protect all parties from security control weaknesses thereby decreasing the risk of compromising the confidentiality, integrity, and availability of the data the interconnected systems store, process, or transmit.

To assist the NCUA in ensuring that external system interconnection agreements are kept up to date, we recommend that NCUA management:

***FY 2022 Recommendation 1:*** *Enforce the process to validate that expired MOUs and those expiring are prioritized for review, update, and renewal in accordance with NCUA policy.*

#### **Agency Response:**

The NCUA agrees. In September 2022, the expiration dates for all authorized external system interconnection agreements, or MOUs, have been added to the NCUA's Governance, Risk, and Compliance (GRC) tool. We will track all such agreements and MOUs in the GRC tool, which will

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

send automated email notifications to information systems security officers (ISSOs) and others in the chain of responsibility well in advance of an agreement or MOU expiring. The agency will ensure these are acted on timely, including addressing any currently expired agreements or MOUs.

**OIG Response:**

We concur with management's planned action.

## Security Function: Protect

---

### 2. The NCUA Needs to Strengthen its Vulnerability Management Program.

#### FY 2022 Core Metrics Domain: *Configuration Management*

We conducted independent vulnerability scans utilizing Nessus. Using the vulnerability data from the Common Vulnerability Scoring System (CVSS<sup>15</sup>) used by Nessus, we identified unpatched software, unsupported software, and improper configuration settings that exposed the NCUA Headquarters network to critical<sup>16</sup> and high<sup>17</sup> severity vulnerabilities. In addition, NCUA did not resolve critical and high-risk vulnerabilities within 30 days of occurrence and medium risk<sup>18</sup> vulnerabilities within 60 days, as required by its internal operating policies. Furthermore, NCUA did not timely remediate older vulnerabilities that were publicly known before 2022.

We conducted independent vulnerability scans during 2018 and made two recommendations<sup>19</sup> and conducted additional scans in 2020<sup>20</sup> and 2021<sup>21</sup> with similar results. NCUA has been working to resolve these recommendations; however, the overall deployment of vendor patches, especially older patches, and system upgrades to mitigate the vulnerabilities continues to be inconsistent, and the 2018 recommendations remain unresolved.

The NCUA Office of Chief Information Officer (OCIO) management stated much of the challenge to making any significant improvement from prior years is due to limited resources to perform the associated functions. Specifically, management stated that the resources to perform vulnerability remediation and other information system operational priorities continues to be a challenge because these same resources are also tasked with operational maintenance and implementation of current and strategic initiatives.

In addition, our scans indicated NCUA's operational environment contains a wide variety of differing technologies. This wide variety of technology compounds NCUA's challenge of having sufficient resources to timely manage and improve its process of mitigating security vulnerabilities and ultimately maturing its overall vulnerability management program.

The *OCIO 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

---

<sup>15</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>16</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>17</sup> High vulnerabilities possess a CVSS rating of 7 to 9.9.

<sup>18</sup> Medium vulnerabilities possess a CVSS rating of 4 to 6.9.

<sup>19</sup> Ibid 9.

<sup>20</sup> *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2020* (OIG Report No. OIG-20-09 November 16, 2020), pg. 8.

<sup>21</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), pg. 7.



**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

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, security 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.

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.

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.

To help NCUA resolve these long-standing recommendations and to assist the agency with maturing its vulnerability management program and ultimately improving its overall security posture, we recommend that management:

***FY 2022 Recommendation 2: 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.***

**Agency Response:**

As part of the 2022 budget, the NCUA commissioned an independent review of the structure and staffing level of OCIO, with a particular emphasis on information security. We expect to have the results of this review soon and will carefully consider the review's conclusions and recommendations and ensure the appropriate allocation of resources to this important function.

NCUA's entire response to Recommendation 2 is provided in Appendix IV.

**OIG Response:**

We concur with management's planned action.

***FY 2022 Recommendation 3: 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.***



**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Agency Response:**

As part of the annual budget and Information Technology Oversight Council processes, the NCUA will continue to evaluate technologies and consolidate them as appropriate. These reviews, decisions, and related plans will be documented. The NCUA will ensure sufficient resources are allocated to supporting the range of technologies adopted to meet the mission and strategies of the agency.

NCUA's entire response to Recommendation 3 is provided in Appendix IV.

**OIG Response:**

We concur with management's planned action.

**3. The NCUA Needs to Require Multifactor Authentication to the NCUA Network for All Privileged and Non-Privileged Users.**

**FY 2022 Core Metrics Domain:** *Identity and Access Management*

(b) (7)(E) non-privileged network users did not use multifactor authentication. Management stated that since the COVID-19 pandemic began in 2020, NCUA has been unable to distribute Personal Identity Verification (PIV) cards in a timely manner, resulting in certain users not having multifactor authentication enabled. In response to the 2021 FISMA audit recommendation to address this issue<sup>22</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.<sup>23</sup>

In addition, (b) (7)(E)

Management informed us the agency does not have a privileged access management solution to address multifactor authentication for shared privileged accounts.<sup>24</sup>

NIST SP 800-53, Revision 5, security control IA-2, Identification and Authentication (Organizational Users) requires organizations to implement multi-factor authentication for access to non-privileged and privileged accounts.<sup>25</sup>

OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, issued May 21, 2019, states: "Agencies shall require PIV credentials (where applicable in accordance with OPM requirements) as the primary means of identification and authentication to Federal information systems and Federally controlled facilities and secured areas by Federal employees and contractors."

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

---

<sup>22</sup> Ibid 11.

<sup>23</sup> In order for CLA to meet their contractual requirement of July 28, 2022 for the draft FISMA reporting metrics, the cutoff date for NCUA to provide evidence for closure of prior year recommendations that were tied to the FY 2022 Core Metrics was June 30, 2022. Therefore, CLA did not assess whether NCUA remediated this issue after June 30, 2022.

<sup>24</sup> (b) (7)(E)  
however, we did not validate this.

<sup>25</sup> IA-2, Identification and Authentication (Organizational Users), Control Enhancements 1 and 2.

## NATIONAL CREDIT UNION ADMINISTRATION FY 2022 FISMA EVALUATION

or personally identifiable information is decreased. Furthermore, privileged accounts are targeted by malicious actors for gaining unauthorized access to system files and data such as system configuration changes, modifying user accounts, and accessing confidential information. Implementing multifactor authentication for privileged access including for shared accounts can decrease the risk of misuse of privileged accounts.

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

To assist NCUA with multi-factor authentication for privileged users, we recommend that NCUA management:

***FY 2022 Recommendation 4: Implement a solution that resolves the privileged access management vulnerability.***

### **Agency Response:**

The NCUA will address this vulnerability. The new laptops to be issued from February 2023 through June 2023 will provide a different capability to restore a laptop that is not properly functioning due to software or configuration issues. This new capability will not rely on a privileged administrator account.

NCUA's entire response to Recommendation 4 is provided in Appendix IV.

### **OIG Response:**

We concur with management's planned action.

## **4. The NCUA Did Not Automatically Disable Inactive Rainy Day SmartPayables User Accounts in Accordance with NCUA Policy.**

### **FY 2022 Core Metrics Domain: *Identity and Access Management***

NCUA did not implement an automated process to disable inactive Rainy Day SmartPayables user accounts after 30 days of inactivity in accordance with NCUA policy. As a result, out of the total population of 11 user accounts, NCUA did not disable three accounts that had been inactive for 30 days or more.

Management specified that Rainy Day SmartPayables requires specific users to process or view the Liquidation file for SmartPayables Mailing Services, which is an infrequent activity and may not require these users to login to their accounts for a period of 30 days or more. Management informed us that to re-enable these automatically disabled accounts would cause an administrative burden on the system administrators and could impact the NCUA in fulfilling specific duties, specifically timely paying depositors their insured deposits from a failed credit union timely.

In response to the auditors notifying management of this issue during the audit, management documented and approved a risk acceptance on July 18, 2022, that details compensating account management controls. We did not validate the compensating controls.

## NATIONAL CREDIT UNION ADMINISTRATION FY 2022 FISMA EVALUATION

NIST SP 800-53, Revision 5, security 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 organization-defined procedures or conditions;
- Support the management of system accounts using organization-defined automated mechanisms.<sup>26</sup>
- Disable accounts within the organization-defined time period when the accounts have been inactive for the organization-defined time-period.<sup>27</sup>

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

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.

Since management has documented and approved a formal acceptance of risk, we are not making a recommendation.

---

<sup>26</sup> AC-2, Account Management, Control Enhancement 1.

<sup>27</sup> AC-2, Account Management, Control Enhancement 3.

# 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>28</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 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 DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On December 6, 2021, OMB issued Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for federal agencies to report to OMB and, where applicable, DHS. Accordingly, the FY 2022 Core Metrics provided reporting requirements across

---

<sup>28</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 2022 FISMA EVALUATION**

**Appendix I**

key areas to be addressed in the independent assessment of agencies' information security programs.<sup>29</sup>

The FY 2022 Core 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, as highlighted in **Table 3**.

**Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2022 IG FISMA Metric Domains**

Cybersecurity Framework Security Functions	Domains in the FY 2022 Core 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 2022 Core 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*.

**Table 4: IG Evaluation Maturity Levels**

Maturity Level	Maturity Level Description
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.

<sup>29</sup> [https://www.cisa.gov/sites/default/files/publications/FY\\_2022\\_Core\\_OIG\\_FISMA\\_Metrics\\_Evaluation\\_Guide\\_\(05-12-22\).pdf](https://www.cisa.gov/sites/default/files/publications/FY_2022_Core_OIG_FISMA_Metrics_Evaluation_Guide_(05-12-22).pdf)

# OBJECTIVE, SCOPE, AND METHODOLOGY

## Objective

The objectives of this performance audit were to (1) assess the NCUA's compliance with FISMA and agency information security and privacy policies and procedures; and (2) respond to the OMB Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines* (FY 2022 Core Metrics).

## Scope

We conducted this performance audit in accordance with general 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 objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

Consistent with our audit objectives, the scope of the audit included assessing select NIST SP 800-53, Revision 5, security and privacy controls mapped to the following FY 2022 Core Metrics domains for four NCUA information systems:

- Risk Management
- Supply Chain Risk Management
- Configuration Management
- Identity and Access Management
- Data Protection and Privacy
- Security Training
- Information Security Continuous Monitoring
- Incident Response
- Contingency Planning

The following four NCUA information systems were selected for review from the 47 internal and external information systems in the NCUA's system inventory as of February 2022:

- General Support System (GSS)
- Modern Examination and Risk Identification Tool (MERIT)
- Financial Disclosure Management System (FDM)
- Rainy Day SmartPayables

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix II**

An internal network vulnerability assessment was also conducted at the NCUA Headquarters. The audit also included a follow up on prior year FISMA audit recommendations to determine if the NCUA made progress in implementing the recommended improvements concerning its information security program.<sup>30</sup>

Audit fieldwork covered NCUA's Headquarters located in Alexandria, VA, from March 30, 2022, to September 14, 2022. The scope of the audit covered the period from October 1, 2021, through September 30, 2022.

## **Methodology**

To determine if the NCUA implemented an effective information security program, we conducted interviews with NCUA officials and reviewed legal and regulatory requirements stipulated in FISMA. Also, we reviewed documents supporting the information security program. These documents included, but were not limited to, the NCUA's (1) information security policies and procedures; (2) incident response procedures; (3) security assessment authorizations; and (4) system generated account listings. Where appropriate, we compared documents, such as the NCUA's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, we performed tests of system processes to determine the adequacy and effectiveness of those controls.

In addition, our work in support of the audit was guided by applicable NCUA policies and federal criteria, including, but not limited to, the following:

- OMB Memorandum M-22-05, *Fiscal Year 2021-2022 Guidance on Federal Information Security and Privacy Management Requirements*.
- OMB Office of the Federal Chief Information Officer *FY 2022 Core IG Metrics Implementation Analysis and Guidelines*.
- Council of the Inspectors General on Integrity and Efficiency, OMB, DHS, and the Federal Chief Information Officers and Chief Information Security Officers councils *FY 2022 Core IG FISMA Metrics Evaluation Guide*.
- NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework).
- OMB Circular No. A-130, *Managing Information as a Strategic Resource*.
- NIST Special Publication 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*.
- NIST Special Publication 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*.
- NIST Special Publication 800-53B, Revision 5, *Control Baselines for Information Systems and Organizations*.
- NIST Special Publication 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*.
- Government Accountability Office *Government Auditing Standards*, April 2021.

---

<sup>30</sup> Ibid 6.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix II**

We selected four information systems from the total population of 47 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 GSS was selected based on risk since it is categorized as a moderate impact system<sup>31</sup> and supports NCUA applications that reside on the network. The MERIT application was selected because it replaced the Automated Integrated Regulatory Examination System as the system of record for credit union exams. FDM is a web-based Army electronic filing system for authorized users to file and maintain required financial interest reports. NCUA uses FDM to track employee's investment information to determine potential conflicts of interest and was selected because it houses employees' personally identifiable information such as social security numbers, and sensitive financial information. Rainy Day SmartPayables was selected because it is a contractor system used by the NCUA Asset Management and Assistance Center for check (payment) printing and mailing services. It is a web-based application with integrated business intelligence analytics and data integration with NCUA's legacy systems. We tested the four systems' selected security controls to support our responses to the FY 2022 Core Metrics.

In testing the effectiveness of 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, this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and, if projected, may be misleading.

---

<sup>31</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>32</sup> 2019,<sup>33</sup> and 2021<sup>34</sup> FISMA audits. During FY 2022, the NCUA implemented corrective actions to close two prior year recommendations.

Audit Year and Recommendation Number	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.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until December 31, 2022.
<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	Open	Open

<sup>32</sup> Ibid 4.

<sup>33</sup> Ibid 5.

<sup>34</sup> Ibid 6.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix III**

<b>Audit Year and Recommendation Number</b>	<b>Status Determined by NCUA</b>	<b>Auditor Position on Status of Recommendation</b>
configurations for all platforms in the NCUA information technology environment in compliance with established NCUA security standards. This includes documenting approved deviations from the configuration baselines with business justifications.		Based on the corrective action plan provided by NCUA management, corrective actions are not 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 are not scheduled for completion until December 2022.
<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  Based on the corrective action plan provided by NCUA management, corrective actions were not scheduled for completion until July 2022. <sup>35</sup>
<b>2021-3:</b> Implement automatic disabling of inactive Salesforce Call Center user accounts for DOCA users in accordance with NCUA policy.	Closed	Closed
<b>2021-4:</b> Document and approve a formal acceptance of risk for not disabling Salesforce inactive accounts after 30 days in accordance with NCUA policy for users whose business needs do not require regular access to the system.	Closed	Closed
<b>2021-5:</b> Complete and issue policies to implement the CUI program.	Open	Open  Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until December 2022.
<b>2021-6:</b> Upon issuance of the CUI policies, design and implement media marking to designate protection	Open	Open

<sup>35</sup> Ibid 23.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix III**

<b>Audit Year and Recommendation Number</b>	<b>Status Determined by NCUA</b>	<b>Auditor Position on Status of Recommendation</b>
standards for safeguarding and/or disseminating agency information.		Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until December 2022.
<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.

NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION

Appendix IV

# MANAGEMENT COMMENTS



National Credit Union Administration  
Office of the Executive Director

SENT BY EMAIL

**TO:** Inspector General James Hagen  
**FROM:** Executive Director Larry Fazio LARRY FAZIO  
**SUBJ:** FISMA Act of 2014 Fiscal Year 2022 Audit Draft Report  
**DATE:** October 20, 2022

Digitally signed by  
LARRY FAZIO  
Date: 2022.10.20  
15:02:32 -04'00'

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) 2022*. We are pleased with the audit's overall conclusion. 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 and maturity level by function, with all functions being rated at level 4 or higher, reflect the commitment the NCUA has made to strong information security.

The draft report makes four 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**

Enforce the process to validate that expired Memorandums of Understanding (MOUs) and those expiring are prioritized for review, update, and renewal in accordance with NCUA policy.

**Management Response:** The NCUA agrees. In September 2022 the expiration dates for all authorized external system interconnection agreements, or MOUs, have been added to the NCUA's Governance, Risk, and Compliance (GRC) tool. We will track all such agreements and MOUs in the GRC tool, which will send automated email notifications to information systems security officers (ISSOs) and others in the chain of responsibility well in advance of an agreement or MOU expiring. The agency will ensure these are acted on timely, including addressing any currently expired agreements or MOUs.

## **Recommendation #2**

Conduct a workload analysis within the Office of the Chief Information Officer (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.

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix IV**

Management Response: As part of the 2022 budget, the NCUA commissioned an independent review of the structure and staffing level of OCIO, with a particular emphasis on information security. We expect to have the results of this review soon and will carefully consider the review's conclusions and recommendations and ensure the appropriate allocation of resources to this important function.

Please note that since March of 2021 the NCUA Office of the Executive Director (OED) has worked closely with OCIO to address the level of outstanding unpatched or unsupported software. Additional resources were added for this function in 2021. The additional resources and emphasis resulted in a significant decline in the level of unpatched or unsupported software. Further, most of the remaining vulnerabilities are primarily related to key legacy systems scheduled for decommissioning or platform upgrades, or systems that are part of ongoing remediation with compensating controls and enhanced monitoring.

The agency has an inventory and detection capability for all installed software. Additionally, the NCUA has a rigorous and repeatable process using a phased approach to identify, acquire, test, and install software patches and updates. Prior to deployment of software and system patches, NCUA thoroughly tests all patches to ensure uninterrupted service and reliability of NCUA systems.

For clarity, we would note that we do not believe we have missed any patches, unsupported software, or improper configuration settings. We have a sound process to identify vulnerabilities and to either remediate the software or settings within the policy timeframes or establish a plan of action and milestone (POAM) and/or acceptance of risk (AOR). POAMs and AORs are only used after carefully considering the residual risk when other mitigations are applied and when replacement or update of the software or settings necessitates more time to acquire, test, and apply without causing significant disruption to agency systems and operations.

The NCUA has a sound risk evaluation and risk acceptance process. The AOR includes a detailed explanation of the need for risk acceptance and the compensating controls that will be used to mitigate the risk during the period of exposure, and AORs are regularly re-evaluated. Compensating controls include several layers of defense from the perimeter to the endpoint designed to detect and protect the network from unauthorized access and the exploitation of any vulnerabilities.

We believe that what the report characterizes as "improper" configuration settings relate to changes to configuration settings due to recently published vulnerabilities or previously acceptable technologies. The reported configuration vulnerabilities are outstanding because of planning required for an alternative strategy after we had to back-out the remediations when they caused a problem with agency services. These are part of ongoing efforts to incrementally implement configuration changes while minimizing the impact to business operations. All are the subject of POAMs and AORs with compensating controls and enhanced monitoring in place to mitigate and monitor ongoing risk.

The NCUA has a rigorous change and configuration management process that has matured over time. In general, to ensure new systems are deployed and configured securely, NCUA

**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix IV**

processes include operational testing, security assessments, and backout plans. Specifically, standard server and endpoint builds are baselined and automatically deployed using configurations from a policy repository or via scripting, thereby creating consistency and greatly reducing the opportunity for human error. The configuration and change operational process includes testing, security impact assessments, backout plans, and tracking of all enterprise system configurations in a central repository. Changes to secure systems are rolled into the system baselines and become standard configuration settings for new systems. In existing systems that are impacted by a new vulnerability discovery, changes are managed in the change and configuration control process which includes vulnerability remediation. Secure system configurations are first installed in test and development environments prior to being deployed to production systems.

External organizations also monitor the NCUA and conduct reviews, including the Department of Homeland Security (DHS) Cybersecurity and Infrastructure Security Agency High Value Asset Assessments, DHS Cyber Hygiene vulnerability scans, and independent third-party penetration testers.

**Recommendation #3**

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.

Management Response: As part of the annual budget and Information Technology Oversight Council processes, the NCUA will continue to evaluate technologies and consolidate them as appropriate. These reviews, decisions, and related plans will be documented. Please note the NCUA's mission spans operating a federal agency, managing asset management estates of failed credit unions, and partnering with state regulatory agencies. This requires a relatively wide range of technological capabilities. The NCUA will ensure sufficient resources are allocated to supporting the range of technologies adopted to meet the mission and strategies of the agency.

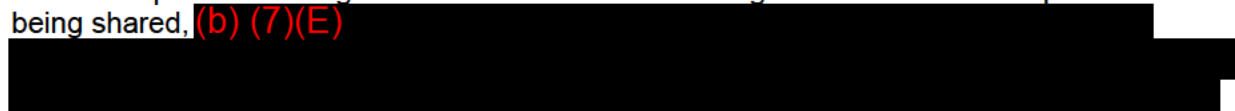
While the number of disparate technologies creates complexity, the NCUA manages an approved software list and reviews, prior to approval, all software requests to reduce or eliminate any unnecessary redundancy.

**Recommendation #4**

Implement a solution that resolves the privileged access management vulnerability.

Management Response: The NCUA will address this vulnerability. The new laptops to be issued from February 2023 through June 2023 will provide a different capability to restore a laptop that is not properly functioning due to software or configuration issues. This new capability will not rely on a privileged administrator account.

In the interim, the NCUA views this vulnerability as relatively low risk given the compensating controls in place. To mitigate the risk associated with single local administrator passwords being shared, (b) (7)(E)





**NATIONAL CREDIT UNION ADMINISTRATION  
FY 2022 FISMA EVALUATION**

**Appendix IV**

(b) (7)(E)

Furthermore, the use of the shared password is limited to a single machine which requires end user permission and participation for an administrator to access the machine locally

(b) (7)(E)

II administrative activities are logged. Finally, prior to joining the NCUA all administrators are thoroughly vetted.

As for multi-factor authentication for all users, the NCUA has been testing a back-up multi-factor solution for when the PIV is not available – such as for new hires, PIV lockouts, and certificate expirations. This back-up solution will be deployed beginning in December 2022. In the interim the NCUA has implemented enhanced monitoring for all internal users temporarily operating without a PIV logon.

**Inactive Rainy Day SmartPayables User Accounts**

Due to limitations with the vendor to configure a multi-customer process to disable inactive accounts after 30 days, an acceptance of risk was signed. Additionally, mitigating controls are in place that result in a low residual risk for this system.

**Status of Prior Year Recommendations**

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

Please contact Deputy Executive Rendell Jones if you have any questions.

Attachment

cc: NCUA Board Members  
DED Jones