**NATIONAL CREDIT UNION ADMINISTRATION
FEDERAL INFORMATION SECURITY MODERNIZATION
ACT OF 2014 AUDIT—FISCAL YEAR 2021**

**Report #OIG-21-09
November 22, 2021**

National Credit Union Administration

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 2021
DATE:	November 22, 2021

Attached is the Office of the Inspector General's FY 2021 independent evaluation of the effectiveness of the National Credit Union Administration's (NCUA) information security program and practices.[1]

The OIG engaged CliftonLarsonAllen LLP (CLA) to perform this evaluation.[2] 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 seven 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.

---

[1] FISMA 2014, Public Law 113-283, requires Inspectors General to perform annual independent evaluations to determine the effectiveness of agency information security programs and practices.
[2] CLA is an independent certified public accounting and consulting firm.

Distribution List:
Chairman Todd M. Harper
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 Samuel Schumach
Chief Information Officer Robert Foster
Chief Financial Officer Eugene Schied
Regional Director and AMAC President Keith Morton
E&I Director Myra Toeppe
CURE Director Martha Ninichuk
OHR Director Towanda Brooks
OCSM Director Kelly Gibbs
OBI Director Kelly Lay
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 2021

Final Report

November 19, 2021

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 (FISMA) for the fiscal year 2021.

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

Controlled Unclassified Information

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) 2021 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 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 Department of Homeland Security's (DHS) *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), dated May 12, 2021.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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, Inspectors General were required to assess 66 metrics in five security function areas — Identify, Protect, Detect, Respond, and Recover that included nine domains — 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*.

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 the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for a sample of four systems in NCUA's inventory of information systems.

Audit fieldwork covered NCUA's headquarters located in Alexandria, VA, from June 9, 2021 to October 20, 2021, assessing the period from October 1, 2020, through September 30, 2021.

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 weaknesses in six of the nine domains in the FY 2021 IG FISMA Reporting Metrics. As a result, we are making seven recommendations to

assist NCUA in strengthening its information security program. In addition, five 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 status. The information included in this report was obtained from NCUA on or before November 19, 2021. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to November 19, 2021.

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

CliftonLarsonAllen LLP

Arlington, Virginia
November 19, 2021

NATIONAL CREDIT UNION ADMINISTRATION
FY 2021 FISMA EVALUATION

TABLE OF CONTENTS

EXECUTIVE SUMMARY

The National Credit Union Administration's (NCUA) Office of Inspector General (OIG) engaged CliftonLarsonAllen LLP (CLA) to conduct a performance audit in support of the Federal Information Security Modernization Act of 2014[1] (FISMA or the Act) 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 Department of Homeland Security's (DHS) *Fiscal Year (FY) 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), dated May 12, 2021.

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. Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST) have issued guidance for federal agencies to follow.

The FY 2021 IG FISMA Reporting Metrics requires us to assess the maturity of five function areas in the NCUA's information security program and practices. For this year's review, IG's were required to assess 66 metrics in 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.[2] 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*.

For this audit, we reviewed selected controls from NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* mapped to the IG FISMA Reporting Metrics for a sample 4 of 41 information systems in the NCUA's information system inventory. We also completed follow-up on prior open FISMA recommendations.

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). 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.

---

[1] FISMA (Public Law 113–283—December 18, 2014) amended the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the OMB with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

[2] The function areas are further broken down into nine domains.

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 2021 IG FISMA Reporting Metrics.[3] All five Cybersecurity Framework Function areas were determined to be at the *Managed and Measurable* (Level 4) maturity level, a significant improvement from *Defined* (Level 2) in FY 2020.[4]

Table 1: Maturity Levels for FY 2021 IG FISMA Reporting Metrics

Security Function	Maturity Level by Function	IG FISMA Metric Domains	Maturity Level by Domain
Identify	Managed and Measurable (Level 4)	**Risk Management**	Managed and Measurable (Level 4)
		Supply Chain Risk Management	Ad-Hoc (Level 1)[5]
Protect	Managed and Measurable (Level 4)	**Configuration Management**	Defined (Level 2)
		Identity and Access Management	Defined (Level 2)
		Data Protection and Privacy	Managed and Measurable (Level 4)
		Security Training	Managed and Measurable (Level 4)
Detect	Managed and Measurable (Level 4)	**Information Security Continuous Monitoring**	Managed and Measurable (Level 4)
Respond	Managed and Measurable (Level 4)	**Incident Response**	Managed and Measurable (Level 4)
Recover	Managed and Measurable (Level 4)	**Contingency Planning**	Managed and Measurable (Level 4)
Overall Rating	**Managed and Measurable (Level 4) Effective**		

---

[3] In accordance with the FY 2021 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.

[4] *FY 2020 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit*, (OIG Report No. OIG-20-09 November 16, 2020), pg. 2.

[5] The FY 2021 IG FISMA Reporting Metrics indicated that, to provide agencies with sufficient time to fully implement NIST Special Publication 800-53, Revision 5, in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating, and therefore would not be considered for the overall rating.

In addition, NCUA took corrective action to close 6 of the 11 prior FISMA open recommendations from the FY 2018,[6] FY 2019,[7] and FY 2020[8] 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 six weaknesses that fell in the supply chain risk management, configuration management, identity and access management, data protection and privacy, and incident response domains of the FY 2021 IG FISMA Metrics (see Findings 1 through 6 in **Table 2**) and have made seven recommendations to assist NCUA in strengthening its information security program. **Table 2** also includes weaknesses where NCUA has five 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 2021 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2021 IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2021 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	The NCUA needs to properly manage unauthorized software on the agency's network. (**Open prior year recommendation**)[9]
	Supply Chain Risk Management	The NCUA needs to enhance its Supply Chain Risk Management (SCRM) strategy, policies, and procedures. (**Finding 1**)
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 platforms. (**Finding 2 (Repeat) & Open prior year recommendations (2)**)[10]
		The NCUA needs to implement standard baseline configuration settings in accordance

---

[6] *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).

[7] *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit – Fiscal Year 2019* (Report No. OIG-19-10, December 12, 2019).

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

[9] 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).

[10] 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).

Cybersecurity Framework Security Function	FY 2021 IG FISMA Reporting Metrics Domain	Weaknesses Noted
		with NIST requirements and NCUA policy. (**Open prior year recommendation**)[11]
	Identity and Access Management	The NCUA needs to require multifactor authentication to the NCUA network for all non-privileged users. (**Finding 3**)
		The NCUA needs to automatically disable inactive Salesforce Call Center user accounts in accordance with NCUA policy. (**Finding 4**)
		The NCUA needs to complete background re-investigations. (**Open prior year recommendation**)[12]
	Data Protection and Privacy	The NCUA needs to implement media marking controls. (**Finding 5**)
	Security Training	None
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	The NCUA needs (b) (7)(E) ▮▮▮▮▮ . (**Finding 6**)
Recover	**Contingency Planning**	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 comments.

---

[11] 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).

[12] 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).

FISMA Audit Findings

Security Function: Identify

1. The NCUA Needs to Enhance its Supply Chain Risk Management Strategy, Policies, and Procedures

FY 2021 IG FISMA Metrics Domain: *Supply Chain Risk Management*

NCUA did not fully address the management of supply chain risks in their SCRM Plan, policies, and procedures. Specifically, we noted that:

- Although the *NCUA Supply Chain Risk Management Plan* includes an introduction to enterprise risk management, it did not address SCRM risk appetite and tolerance, processes for monitoring supply chain risk, and associated SCRM controls.

- The *NCUA Acquisition Policy Manual, Procedures and Requirements for NCUA Acquisitions* did not address the following:

  o Roles and responsibilities, and procedures specifically related to facilitating the implementation of the SCRM Plan.
  o Procedures to detect and prevent counterfeit components from entering the system, and requirements and procedures for reporting counterfeit system components.
  o Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.
  o Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers.
  o Tools and techniques to utilize the acquisition process to protect the supply chain, including, risk-based processes for evaluating cybersecurity supply chain risks associated with third party providers, as appropriate.
  o Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.

NCUA management did not perform a detailed review of SCRM NIST guidance and update the SCRM plan, policies, and procedures to fully address the management of supply chain risks.

Public law 115-390 – 115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act* or the "SECURE Technology Act" (December 31, 2018) requires executive agencies to develop an overall SCRM strategy and implementation plan and policies and processes to guide and govern SCRM activities.

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations,* April 2015, provides guidance to federal agencies on identifying, assessing, selecting, and implementing risk management processes and mitigating controls throughout their organizations to help manage information and communications technology (ICT) supply chain risks. It addresses the following regarding SCRM practices and controls:

- Selecting and tailoring SCRM controls based on i) the environment in which information systems are acquired and operate; (ii) the nature of operations conducted; (iii) the types of threats facing the organization, missions/business processes, supply chains, and information systems; and (iv) the type of information processed, stored, or transmitted by information systems and the supply chain infrastructure.

- Implementing acquisition strategies, tools, and methods to ensure the integrity and traceability of ICT supply chain infrastructure and supply systems/components.

- Employing tailored acquisition strategies, contract tools, and procurement methods for purchasing information systems, system components, or information system services from suppliers.

- Implementing anti-counterfeit policies and procedures as means to help ensure that the components acquired and used are authentic and have not been subject to tampering.

- Managing risks associated with component repair including the repair process and any replacements, updates, and revisions of hardware and software components within the ICT supply chain infrastructure.

With a fully developed and implemented SCRM strategy and related policies and procedures, NCUA personnel can better identify and reduce the risk of unanticipated, and therefore unmitigated, supply chain risks.

To assist the NCUA in strengthening supply chain risk management controls we recommend that NCUA management:

> *FY 2021 Recommendation 1: Review the SCRM NIST guidance and update the SCRM plan, policies, and procedures to fully address supply chain risk management controls and practices.*
>
> **Agency Response:**
> In accordance with NIST SP 800-161, the NCUA will update the Supply Chain Risk Management (SCRM) plan, policies, and procedures to fully address SCRM controls and practices. The estimated completion date is December 2022.
>
> **OIG Response:**
> We concur with management's planned action.

Security Function: Protect

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

FY 2021 IG FISMA Metrics Domain: *Configuration Management*

Using vulnerability data from the Common Vulnerability Scoring System (CVSS[13]) used by Nessus, we identified unpatched software, unsupported software, and improper configuration settings that exposed the NCUA Headquarters (HQ) network to critical[14] and high[15] severity vulnerabilities. In addition, NCUA did not resolve critical and high-risk vulnerabilities within 30 days of occurrence and medium risk[16] vulnerabilities within 60 days, as required by its internal operating policies. Furthermore, NCUA did not remediate older vulnerabilities that were publicly known before 2021, in a timely manner.

We observed that NCUA had made some improvements in its vulnerability management processes since 2018. Compared to our vulnerability scans of the NCUA's network in 2018, we observed improvement in the total[17] number of critical and high vulnerabilities per host.[18] Specifically, there are 17 percent fewer total vulnerabilities per host and nine percent fewer total unique vulnerabilities per host.[19] However, issues remain with applying older patches and remediating older configuration weaknesses.

The overall deployment of vendor patches, especially older patches, and system upgrades to mitigate the vulnerabilities continues to be inconsistent. NCUA Office of Chief Information Officer (OCIO) management stated that managing resources to perform vulnerability remediation and other information system operational priorities continues to be challenging.

In addition, our scan results identified older vulnerabilities that did not appear in NCUA's scan reports from March 2021, indicating that the agency's vulnerability scanning process did not fully capture the vulnerabilities. OCIO management stated that 39 assets were moved as part of OCIO's efforts to segment the network for greater protection and isolation, and these assets were not scanned.

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 days, after which a POA&M must be established.

---

[13] 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.

[14] 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.

[15] High vulnerabilities possess a CVSS rating of 7 to 9.9.

[16] Medium vulnerabilities possess a CVSS rating of 4 to 6.9.

[17] Total vulnerabilities include all vulnerabilities identified regardless of the age of the vulnerability.

[18] We performed vulnerability assessments for the fiscal year 2018 and 2021 FISMA audits in accordance with our contract with the NCUA OIG.

[19] There were 48 more hosts included in the credential scans this year (476) than were included in the 2018 scans (428).

- 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 4, 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 installing required patches in a timely manner, implementing secure configuration settings, and migrating to supported software, NCUA can mitigate the security weaknesses and limit the ability of attackers to compromise the confidentiality, integrity, and availability of data. This ultimately will improve the overall security posture of NCUA information systems.

The FY 2018 FISMA Audit Report included recommendations[20] to ensure the Chief Information Officer (CIO) enforces the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes; and implement a process to detect and migrate unsupported software to supported platforms before support for the software ends. NCUA had not migrated the unsupported software to supported platforms and did not meet agency defined timeframes for remediation of critical and high vulnerabilities. These recommendations will remain open until we have validated that NCUA has fully implemented them; therefore, we are not making any new recommendations.

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

FY 2021 IG FISMA Metrics Domain: *Identity and Access Management*

NCUA did not require multifactor authentication (MFA) to the NCUA network for 246 non-privileged users.

Management stated that due to the COVID-19 pandemic that began in 2020, staff and contractors experienced delays with Personnel Identity Verification (PIV) card issuance used for MFA due to the closure of federal offices issuing the cards. NCUA OCIO issued an interim policy approving

---

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

the use of Temporary Accounts single factor authentication (username and password) that must be approved by Supervisors and/or Contracting Officer's Representatives at a minimum of every 60 days. Although federal offices issuing PIV cards became more accessible during FY 2021, management stated that PIV multifactor authentication was not enforced for these users due to continued COVID-19 concerns of staff and contractors regarding entering NCUA offices to obtain a PIV card.

Management also stated that DUO, an alternative multifactor authentication token, was not implemented for these users due to the lack of enterprise licenses. Additionally, management stated that a project to use Microsoft Azure Active Directory Multifactor Authentication was underway but was not fully implemented.

NIST SP 800-53, Revision 4, security control IA-2, Identification and Authentication (Organizational Users) requires multifactor authentication for network access to non-privileged accounts.

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."

On March 13, 2020, the CISA (Cybersecurity & Infrastructure Security Agency) issued alert AA20-073A, *Enterprise VPN Security* that encouraged organizations to adopt a heightened state of cybersecurity as they prepared for potential COVID-19 impacts. The Alert stated that organizations that do not use MFA for remote access are more susceptible to phishing attacks. CISA recommends implementing MFA on all virtual private network connections to increase security. If MFA is not implemented, require teleworkers to use strong passwords.

Although CISA recommended the use of strong passwords as a compensating control, multifactor authentication adds an additional layer of security, which is why NIST requires its use. With multifactor authentication a malicious actor must have access to a smart card or a personal identification number (PIN). The NCUA's use of passwords due to the pandemic has been ongoing for 18 months and NCUA management has still not communicated a specific date that these (and new) staff and contractors are required to start using multifactor authentication as the impact of the pandemic continues. The long-term use of passwords provides more time for malicious actors to compromise authentication via phishing attacks.

By requiring multifactor authentication for all NCUA network users, the risk of unapproved access leading to unauthorized modification, loss, and disclosure of sensitive NCUA information or personally identifiable information during extended periods of telework, is decreased. In addition, NCUA information systems are at decreased risk for disruption of operation, enabling staff and contractors to productively support the Agency's mission.

To assist the NCUA in strengthening identification and authentication controls, we recommend that NCUA management:

> **FY 2021 Recommendation 2:** *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.*

Agency Response:
The NCUA will document and implement a plan to deploy multifactor authentication for personnel with a network account without a PIV card. The estimated competition date is July 2022.

OIG Response:
We concur with management's planned action.

4. The NCUA Needs to Automatically Disable Inactive Salesforce Call Center User Accounts in Accordance with NCUA Policy

FY 2021 IG FISMA Metrics Domain: *Identity and Access Management*

NCUA did not implement an automated or manual process to disable inactive Salesforce Call Center (Salesforce) user accounts after 30 days of inactivity in accordance with NCUA policy. As a result, the following accounts were not disabled after 30 days of inactivity:

- 61 NCUA Salesforce users who did not log on for more than 30 days.

- 54 NCUA Salesforce users who never logged in to the system.

Office of Consumer Financial Protection management stated that although NCUA has been using Salesforce since 2015, they just recently became aware of the NCUA policy requiring automatic disabling of inactive accounts. Management also stated that due to their job functions, NCUA examiners, Ombudsmen, Consumer Compliance Policy and Outreach analysts, and Regional Directors only use Salesforce on an ad-hoc basis and therefore do not log into the system on a regular basis. Alternatively, NCUA Division of Consumer Affairs (DOCA) personnel log into Salesforce regularly to perform their job duties. Although NCUA has established a business case for not automatically disabling Salesforce inactive accounts for certain NCUA ad-hoc users, the agency has not documented and approved a formal acceptance of risk.[21]

Management informed us that after it completes a project in February 2022 to implement multifactor authentication, it is planning to begin a project to implement automatic disabling of inactive DOCA user accounts.

NIST SP 800-53, Revision 4, security control AC-2, Account Management requires automatically disabling accounts when the accounts have been inactive for an organization defined time-period.

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

---

[21] According to NIST SP 800-39, *Managing Information Security Risk Organization, Mission, and Information System View*, risk acceptance is an appropriate risk response when the identified risk is within the organizational risk tolerance. Consideration of organizational priorities and trade-offs between mission/business needs and the potential impacts on individuals, other organizations, and the Nation determine the level and types of acceptable risk.

modification, loss, and disclosure of sensitive NCUA information, and reduce the risk of disrupting mission critical agency systems.

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

> *FY 2021 Recommendation 3: Implement automatic disabling of inactive Salesforce Call Center user accounts for DOCA users in accordance with NCUA policy.*
>
> **Agency Response:**
> The NCUA agrees to implement automatic disabling of inactive Salesforce Call Center user accounts for the Division of Consumer Affairs users in accordance with NCUA policy and document and approve a formal acceptance of risk. The estimated completion date is June 2022.
>
> **OIG Response:**
> We concur with management's planned action.
>
> *FY 2021 Recommendation 4: 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.*
>
> **Agency Response:**
> The NCUA agrees to document and approve a formal acceptance of risk and implement automatic disabling of inactive Salesforce Call Center user accounts for the Division of Consumer Affairs users in accordance with NCUA policy. The estimated completion date is June 2022.
>
> **OIG Response:**
> We concur with management's planned action.

5. The NCUA Needs to Implement Media Marking Controls

FY 2021 IG FISMA Metrics Doman: *Data Protection and Privacy*

NCUA has not implemented standards and procedures for marking digital and non-digital information system media.[22]

Management stated that media marking was not implemented because the agency has not completed and published the Controlled Unclassified Information (CUI) policy in accordance with Executive Order 13556[23] and the National Archives and Records Administration (NARA) CUI Notice 2020-01[24] that will guide its media marking standards. Management stated the delay in completing the CUI policy was due to a lack of resources. In addition, NCUA management stated that NARA made significant changes to the CUI categories and NCUA needed additional time to

---

[22] Media marking denotes the use of human-readable security attributes applied to digital and non-digital information used to designate distribution limitations, handling caveats, and applicable security markings.

[23] Executive Order 13556 -- *Controlled Unclassified Information*, issued on November 4, 2010 required agencies to complete and publish their CUI policy.

[24] On May 14, 2020, the NARA Information Security Oversight Office issued CUI Notice 2020-01: *CUI Program Implementation Deadlines* requiring agencies to issue policies by December 31, 2020 that implement the CUI program.

complete the policy. At this time, management has not specified an estimated completion date for completing and issuing the CUI policy.

Although management has not completed the CUI policy, in April 2018, the Agency designated the CUI Senior Agency Official (SAO), assigned the Office of General Counsel Access Law Section the responsibility for administering its CUI program, and committed to providing the CUI SAO with additional resources.

NIST SP 800-53, Revision 4, security control MP-3, Media Marking requires NCUA to mark information system media indicating the distribution limitations, handling caveats, and applicable security markings (if any) of the information; and exempt organization-defined types of information system media from marking as long as the media remain within organization-defined controlled areas.

Implementing a media marking policy will assist NCUA personnel with appropriately protecting sensitive agency information, decreasing the risk of unauthorized access and disclosure.

To assist the NCUA in strengthening data protection and privacy controls, we recommend that NCUA management:

> ***FY 2021 Recommendation 5:*** *Complete and issue policies to implement the CUI program.*
>
> **Agency Response:**
> NCUA will develop and issue a media marking policy by December 31, 2022. The National Archives and Records Administration (NARA) is in the process of revising the CUI Registry. Once NARA completes its modifications to the CUI Registry and the CUI categories, NCUA will incorporate the media marking policy into the broader CUI program, based on the finalized version of NARA's CUI Registry.
>
> **OIG Response:**
> We concur with management's planned action.
>
> ***FY 2021 Recommendation 6:*** *Upon issuance of the CUI policies, design and implement media marking to designate protection standards for safeguarding and/or disseminating agency information.*
>
> **Agency Response:**
> When the policy is issued (by December 31, 2022) the NCUA will implement media marking in accordance with the policy.
>
> **OIG Response:**
> We concur with management's planned action.

Security Function: Respond

6. The NCUA Needs to (b) (7)(E)

FY 2021 IG FISMA Metrics Domain: *Incident Response*

NCUA has not (b) (7)(E)
(b) (7)(E), [26] (b) (7)(E), [27] (b) (7)(E) .

Management stated that it has not (b) (7)(E) because of its
challenge to continuously balance the operational costs for security of a small agency while
adhering to federal requirements in order to protect NCUA data. Management also stated that the
OCIO is in the process of re-evaluating its Security Information and Event Management (SIEM)
technology[28] (b) (7)(E) .
Management decided against investing resources to (b) (7)(E)
(b) (7)(E) in case it is determined to not be the continuing solution for meeting NCUA's
technology needs.

Management stated that (b) (7)(E)
Our testing validated these tools are in place.

NIST SP 800-53, Revision 4, (b) (7)(E)

The *NCUA Information Security Procedural Manual* requires (b) (7)(E)
in accordance with NIST.

(b) (7)(E) , NCUA is able to take
corrective action to remove any suspected malicious code and reduce the risk of substantial
damage related to data loss or manipulation.

To assist the NCUA in strengthening its ability to detect unauthorized changes to software,
firmware, and information, we recommend that NCUA management:

> *FY 2021 Recommendation 7:* (b) (7)(E)
>
> **Agency Response:**
> The NCUA will (b) (7)(E) .
>
> **OIG Response:**
> We concur with management's planned action.

---

[25] (b) (7)(E)
.
[26] Software includes operating systems, middleware, and applications.
[27] Firmware is software stored on hardware designed to make it function properly and includes the Basic Input Output
System (BIOS).
[28] SIEM technology provides real-time analysis of security alerts generated by applications and network hardware.

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,[29] 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 DHS annually provide instructions to federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-21-02, *Fiscal Year 2020-2021 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 2021 IG FISMA Reporting Metrics, provided reporting

---

[29] 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."

requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[30]

The FY 2021 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, as highlighted in **Table 3**.

Table 3: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2021 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	Domains in the FY 2021 IG FISMA Reporting Metrics
Identify	Risk Management, Supply Chain Risk Management[31]
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 2021 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*.

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.

---

[30] https://www.cisa.gov/publication/fy21-fisma-documents
[31] Ibid 5.

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 Department of Homeland Security's (DHS) *FY 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (FY 2021 IG FISMA Reporting Metrics), dated May 12, 2021.

Scope

We conducted this performance audit in accordance with GAGAS. 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.

The scope of the audit included assessing select NIST 800-53, Revision 4, security and privacy controls mapped to the following FY 2021 IG FISMA Reporting 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 41 information systems in the NCUA's system inventory as of June 9, 2021:

- General Support System (GSS)

- Credit Union Service Organization Registry (CUSO Registry)

- HR Links

- Salesforce Call Center

An internal network vulnerability assessment was also conducted at HQ.

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.[32] Audit fieldwork covered NCUA's HQ located in Alexandria, VA, from June 10 to October 20, 2021. The scope of the audit covered the period from October 1, 2020, through September 30, 2021.

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; (4) plans of action and milestones; (5) configuration management plans; and (6) 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:

- FY 2021 IG FISMA Reporting Metrics.

- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.

- 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.

- NIST SP 800-53A*,* Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* for the assessment of security control effectiveness.

- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).

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.

---

[32] Ibid 8.

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,[33] 2019,[34] 2020[35] FISMA audits. During FY 2021, the NCUA implemented corrective actions to close six prior year recommendations.

Audit Year and Recommendation Number	Status Determined by NCUA	Auditor Position on Status of Recommendation
2018-6: 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.
2018-8: 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
2018-9: 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
2018-10: 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.
2019-3: The NCUA management ensures the Agency performs likelihood	Closed	Closed

---

[33] Ibid 6.
[34] Ibid 7.
[35] Ibid 8.

Audit Year and Recommendation Number	Status Determined by NCUA	Auditor Position on Status of Recommendation
analysis on all known vulnerabilities from all sources as part of its information system risk assessment.		
2019-4: 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 established NCUA security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Open	Open Based on the corrective action plan provided by NCUA management, corrective actions are not scheduled for completion until December 31, 2024.
2019-5: The NCUA management ensures the Agency maintains and reviews test results in ServiceNow for all system changes.	Closed	Closed
2019-6: The NCUA management ensures the Agency completes and documents a security impact analysis for emergency changes in accordance with the OCIO Operational Change Control Board Charter.	Closed	Closed
2019-9: The NCUA management ensures the Chief Information Officer develops and implements a process to document and maintain evidence that users sign access agreements prior to accessing the agency's network.	Closed	Closed
2020-1: The NCUA management reviews the timeframe required to complete the Employee Exit Form workflow process in SharePoint and disable access to NCUA information systems for separated employees and contractors; and ensure the same timeframe is documented in the NCUA Information Security Procedural Manual for controls PS-4a and f, and AC-2f.	Closed	Closed
2020-2: The NCUA management develops and implements a monitoring process to ensure the Employee Exit Form process is completed in accordance with the timelines established in NCUA policy.	Closed	Closed

MANAGEMENT COMMENTS

National Credit Union Administration
Office of the Executive Director

OCIO/RF:JD
SSIC: 13500

SENT BY EMAIL

TO: Inspector General, James Hagen

FROM: Executive Director, Larry Fazio

LARRY FAZIO Digitally signed by LARRY FAZIO
Date: 2021.11.16 09:01:00 -05'00'

SUBJ: Audit of the NCUA's information security program and practices in
           accordance with the Federal Information Security Modernization Act of
           2014 (FISMA) for the fiscal year 2021

DATE: November 16, 2021

Thank you for the opportunity to review and comment on the results of the audit of the
NCUA'sinformation security program and practices in accordance with the Federal
Information Security Modernization Act of 2014 (FISMA) Reporting Metrics for fiscal year
2021.

We are pleased with the audit's overall conclusion that the 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.

The FY 2021 audit made seven recommendations to assist NCUA in strengthening
its information security program. Responses to the FY 2021 audit
recommendations and planned corrective actions, as appropriate, are provided
below.

Recommendation 1: Review the SCRM NIST guidance and update the SCRM plan,
policies, and procedures to fully address supply chain risk management controls and
practices.

1775 Duke Street — Alexandria, VA 22314-6113 — 703-518-6320

Controlled Unclassified Information

Management Response: In accordance with NIST SP 800-161, the NCUA will update the Supply Chain Risk Management (SCRM) plan, policies, and procedures to fully address SCRM controls and practices. The estimated completion date is December 2022.

Recommendation 2: 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.

Management Response: The NCUA will document and implement a plan to deploy multifactor authentication for personnel with a network account without a PIV card. The estimated competition date is July 2022.

Recommendation 3: Implement automatic disabling of inactive Salesforce Call Center user accounts for DOCA users in accordance with NCUA policy.

Management Response: The NCUA agrees to implement automatic disabling of inactive Salesforce Call Center user accounts for the Division of Consumer Affairs users in accordance with NCUA policy and document and approve a formal acceptance of risk. The estimated completion date is June 2022.

Recommendation 4: 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.

Management Response: The NCUA agrees to document and approve a formal acceptance of risk and implement automatic disabling of inactive Salesforce Call Center user accounts for the Division of Consumer Affairs users in accordance with NCUA policy. The estimated completion date is June 2022

Recommendation 5: Complete and issue policies to implement the CUI program.

Management Response: NCUA will develop and issue a media marking policy by December 31, 2022. The National Archives and Records Administration (NARA) is in the process of revising the CUI Registry. Once NARA completes its modifications to the CUI Registry and the CUI categories, NCUA will incorporate the media marking policy into the broader CUI program, based on the finalized version of NARA's CUI Registry.

Recommendation 6: Upon issuance of the CUI policies, design and implement media marking to designate protection standards for safeguarding and/or disseminating agency information.

Management Response: When the policy is issued (by December 31, 2022) the NCUA will implement media marking in accordance with the policy.

Recommendation 7: (b) (7)(E) .

Management Response: (b) (7)(E)
(b) (7)(E) .

Thank you for the opportunity to comment.

1775 Duke Street – Alexandria, VA 22314-6113 – 703-518-6320