NCUA
National Credit Union Administration

OFFICE OF INSPECTOR GENERAL

NATIONAL CREDIT UNION ADMINISTRATION
FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT—FISCAL YEAR 2020

Report #OIG-20-09
November 16, 2020

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 2020

DATE: November 16, 2020

Attached is Office of the Inspector General's FY 2020 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 audit report summarizes the results of CLA's independent evaluation and contains two recommendations that will assist the agency in improving the effectiveness of its information security and its privacy programs and practices. NCUA management concurred with and has planned corrective actions to address the recommendations.

We appreciate the effort, professionalism, courtesies, 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 Rodney E. Hood
Board Member J. Mark McWatters
Board Member Todd M. Harper
Executive Director Larry Fazio
Acting General Counsel Frank Kressman
Deputy Executive Director Rendell Jones
Deputy Chief of Staff Gisele Roget
Acting OEAC Deputy Director Joy Lee
Chief Information Officer Robert Foster
Chief Financial Officer Eugene Schied
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
Senior Agency Information Security/Risk Officer David Tillman

Attachment

OIG-20-09

National Credit Union Administration

Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2020

Final Report

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

November 12, 2020

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 2020.

We appreciate the assistance we received from the NCUA and appreciate the opportunity to serve you. 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

CliftonLarsonAllen LLP
CLAconnect.com

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 2020 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA or the Act). FISMA requires agencies to develop, implement, and document an agency-wide information security program and practices. The Act also requires Inspectors General (IG) to conduct an annual independent evaluation of their agencies' information security programs and report the results to the Office of Management and Budget (OMB).

The objective of this performance audit was to assist the NCUA Office of Inspector General (OIG) in assessing the NCUA's compliance with FISMA and agency information security and privacy policies and procedures.

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

The audit included an assessment of the 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 (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for a sample of 4 of 39 systems in NCUA's inventory of information systems. The security controls selected for testing were mapped to the Department of Homeland Security's IG FISMA Reporting Metrics for assessing the maturity of an agency's information security program in eight IG FISMA Metric Domains and five Function Areas.

Audit fieldwork covered NCUA's headquarters located in Alexandria, VA, from June 10 to October 20, 2020.

We concluded that the NCUA has, for the most part, formalized and documented its policies, procedures, and strategies; however, the NCUA faces certain challenges in the consistent implementation of its information security program and practices. While we noted improvements and effective controls related to training, incident response, and contingency planning, we identified weaknesses in three of the eight domains of the FY 2020 IG FISMA Reporting Metrics related to risk management, configuration management, and identity and access management. These control weaknesses effect 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. We have made two new recommendations to assist the NCUA in strengthening its information security program. In addition, 9 of the 21 prior FISMA open recommendations related to the NCUA's security program and practices 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 12, 2020. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to November 12, 2020.

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 12, 2020

TABLE OF CONTENTS

Executive Summary 1

FISMA Audit Findings 6

Security Function: Identify 6

1. The NCUA did not Effectively Implement Controls Over its Agency-Issued Mobile Devices 6

Security Function: Protect 8

2. The NCUA Needs to Remediate Network Vulnerabilities in Accordance with NCUA Policy 8

3. The NCUA Needs to Ensure System Accounts for Separated Personnel are Disabled 10

4. The NCUA Needs to Ensure All Network Users Complete Access Agreements 12

Appendix I – Background 14

Appendix II – Objective, Scope, and Methodology 16

Appendix III – Status of Prior Year Recommendations 18

Appendix IV – Management Comments 22

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 objective of this performance audit was to assist the NCUA OIG in assessing the NCUA's compliance with FISMA and agency information security and privacy policies and procedures.

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 agency information security programs 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. In addition, NIST issued the Federal Information Processing Standards (FIPS) to establish agency baseline security requirements.

Agencies must also report annually to OMB and to congressional committees on the effectiveness of their information security program. OMB and the Department of Homeland Security (DHS) annually provide instructions to federal agencies and IGs for preparing FISMA reports. On November 19, 2019, OMB issued Memorandum M-20-04, *Fiscal Year 2019-2020 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[2] to independently assess their agencies' information security programs.

The fiscal year (FY) 2020 IG FISMA Reporting Metrics are designed to assess the maturity[3] 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. The IG FISMA Metrics consists of 67 objective questions in the five security function areas and further divided into eight domains. Based on the answers, a weighted algorithm contained in the DHS Cyberscope system calculates a maturity score for each domain and security function, and then further rates the maturity of an agency's information security program as a whole. The maturity levels range—from lowest to highest—*Ad Hoc, Defined, Consistently Implemented, Managed and Measurable, and Optimized*. A component must be rated at Level 4 (Managed and Measurable) to be considered effective.

[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] CLA submitted its responses to the FY 2020 IG FISMA Reporting Metrics to the NCUA OIG as a separate deliverable.

[3] The five levels in the maturity model are: Level 1 - *Ad hoc*; Level 2 - *Defined*; Level 3 - *Consistently Implemented*; Level 4 - *Managed and Measurable*; and Level 5 - *Optimized*.

For this audit, CLA 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 4 of 39 information systems in the NCUA's information system inventory as of June 10, 2020. CLA also analyzed the calculated results of the IG FISMA Reporting Metrics and assessed the overall effectiveness of the NCUA's information security program as it pertains to the four NCUA information systems that we tested.

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

Audit Results

According to the objective evaluation of the IG FISMA Reporting Metrics, the NCUA's information security program fell below the specified threshold of effectiveness, *Managed and Measurable* (Level 4) as shown in **Table 1**. The NCUA's information security program achieved an overall rating of *Defined* (Level2). Specifically, three of the five Cybersecurity Framework Function areas were at a *Defined* (Level 2) maturity level and two of the five Cybersecurity Framework Function areas were determined to be at the *Managed and Measurable* (Level 4) maturity level. The maturity metrics for the eight domains and five security functions remain unchanged from FY 2019.

Table 1: Calculated Maturity Levels by Function Area, Domain and Overall for FY 2020

Security Function	Calculated Maturity Level by Function	IG FISMA Metric Domains	Calculated Maturity Level by Domain
Identify	Defined (Level 2)	**Risk Management**	Defined (Level 2)
Protect	Defined[4] (Level 2)	**Configuration Management**	Defined (Level 2)
		Identity and Access Management	Defined (Level 2)
		Data Protection and Privacy	Consistently Implemented (Level 3)
		Security Training	Managed and Measurable (Level 4)
Detect	Defined (Level 2)	**Information Security Continuous Monitoring**	Defined (Level 2)
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 Calculated Rating	**Defined (Level 2) Not Effective**		

[4] The most frequent maturity level rating across the Protect Cybersecurity Framework (CSF) function served as the overall scoring.

The IG FISMA Reporting Metrics also provided the agency IG the discretion to determine the rating for each of the Cybersecurity Framework domains and functions, and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FY 2020 FISMA audit. Although we identified areas for improvement this year, the weaknesses we identified during this year's audit, in combination, do not have a significant enough impact on the NCUA's overall information security program for us to consider it ineffective. We noted that NCUA implemented effective controls and improvements in the following areas:

- Strengthened the Plan of Action and Milestones (POA&Ms) process.
- Implemented a formal privacy continuous monitoring strategy, and a process to measure the effectiveness of privacy activities.
- Maintained an effective program for security awareness training, incident response, and contingency planning.

Along with the improvements noted, the NCUA has, for the most part, formalized and documented its policies, procedures, and strategies; however, the NCUA faces certain challenges in the consistent implementation of its information security program. We identified weaknesses in three of the eight domains of the FY 2020 IG FISMA Reporting Metrics related to risk management, configuration management, and identity and access management (see **Table 2**). 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.

In addition, our review of the prior FISMA recommendations determined that 9 of the 21 prior FISMA open recommendations related to the NCUA's security program and practices remain open. Implementing more of these recommendations will help NCUA to mature its information security program. Refer to **Appendix III** for a detailed description of the status of each recommendation.

The existing weaknesses identified in this audit align with the particular security domains, as summarized in **Table 2**, which details the weaknesses mapped to the IG FISMA Metric Domains. The existing weaknesses include both the findings noted in the FY 2020 FISMA audit and the nine prior years' recommendations that remain open, detailed in Appendix III.

Table 2: Weaknesses Noted in FY 2020 FISMA Audit Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2020 IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2020 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	The NCUA did not effectively implement controls over its agency-issued mobile devices. (**Finding 1**)
		The NCUA did not properly manage unauthorized software on the agency's network. (**Open prior year recommendation**)[5]
		The NCUA did not document and analyze all known control weaknesses in information

[5] 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).

Cybersecurity Framework Security Function	FY 2020 IG FISMA Reporting Metrics Domain	Weaknesses Noted
		system risk assessments. (**Open prior year recommendation**)[6]
Protect	**Configuration Management**	The NCUA did not remediate network vulnerabilities in accordance with NCUA policy. (**Finding 2 & Repeat/Open prior year recommendations**)[7]
		The NCUA did not implement standard baseline configuration settings in accordance with NIST requirements and NCUA policy. (**Open prior year recommendation**)[8]
		The NCUA did not consistently implement information system changes in accordance with NCUA policy. (**Open prior year recommendations**)[9]
	Identity and Access Management	The NCUA did not ensure system accounts for separated personnel were disabled. (**Finding 3**)
		The NCUA did not ensure all network users completed access agreements. (**Finding 4 & Repeat/Open prior year recommendation**)[10]
		The NCUA did not complete background re-investigations. (**Open prior year recommendation**)[11]
	Data Protection and Privacy	None
	Security Training	None
Detect	**Information Security Continuous Monitoring**	None
Respond	**Incident Response**	None
Recover	**Contingency Planning**	None

[6] Recommendation 3, *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit*, (OIG Report No. OIG-19-10, December 12, 2019).

[7] 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).

[8] 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).

[9] Recommendations 5 and 6, *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit*, (OIG Report No. OIG-19-10, December 12, 2019).

[10] Recommendation 9, *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit*, (OIG Report No. OIG-19-10, December 12, 2019).

[11] 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).

We have made two new recommendations to assist the NCUA in strengthening its information security program.

In response to the draft report, the NCUA concurred with the two recommendations, and described its plans to address them. Based on our evaluation of management comments, we acknowledge the NCUA's management planned actions to address the recommendations. The NCUA management comments are included in their entirety in Appendix IV.

The following section provides a detailed discussion of the audit findings. Appendix I provides background information on NCUA and the FISMA legislation, and Appendix II describes the evaluation scope, objective, and methodology.

FISMA Audit Findings

Security Function: Identify

1. The NCUA did not Effectively Implement Controls Over its Agency-Issued Mobile Devices

FY 2020 IG FISMA Metric Area: *Risk Management*

NCUA did not effectively implement controls over its NCUA-issued mobile phones and tablets. Specifically, we noted:

- NCUA did not require users to install security and operating system updates on their mobile phones and tablets within a prescribed period.

- NCUA did not restrict mobile phones and tablets that were not updated within that prescribed period from accessing the NCUA enterprise services.

NCUA tests mobile phone and tablet updates prior to releasing them to all NCUA staff. Once the mobile phone and tablet updates are approved for release, [redacted]. Management stated NCUA previously had the settings configured to not allow mobile phones and tablets to connect to the NCUA network if they were not updated. However, due to issues with users updating and connecting to the network, NCUA disabled this setting.

Upon notification of this issue to management during the audit, in August of 2020, NCUA implemented a configuration change to their mobile device management software to require that all mobile phones and tablets have the most recent security and operating system updates in order to access NCUA's applications. CLA validated the configuration change was implemented.

NIST SP 800-53, Revision 4, security control Access Control (AC)-19, Access Control for Mobile Devices, requires agencies to establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.

NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise,* states that "general security recommendations for any IT technology are provided in NIST SP 800-53, and policy restrictions of particular interest for mobile device security include:"

- Limiting or preventing access to enterprise services based on the mobile device's operating system version.

Across government and the private sector, individuals rely increasingly on mobile devices for official communications and interfacing with office systems and networks. By enforcing compliance with applying security and operating system updates via an automated tool, NCUA is increasing the security of the organization’s data and decreasing the risk of vulnerabilities being exploited on those devices.

Since NCUA remediated the control weakness during the audit, we are not making a recommendation.

Security Function: Protect

2. The NCUA Needs to Remediate Network Vulnerabilities in Accordance with NCUA Policy

FY 2020 IG FISMA Metric Area: *Configuration Management*

Unpatched software, unsupported software, and improper configuration settings exposed the NCUA Headquarters [redacted] Specifically, NCUA's [redacted] between September 15th and October 4th of 2020 [redacted] outside of NCUA's remediation timeframe which related to patch management, configuration management, and unsupported software. These vulnerabilities included:

- [redacted] that h[redacted] been publicly known since prior to March 2020.
- Configuration Weaknesses: belong to groups, and weaknesses [redacted] that [redacted]
- Unsupported Software: The unsupported software on NCUA's network included [redacted] Microsoft ended support on January 14, 2020.

In addition, NCUA did not remediate [redacted] from identification in accordance with NCUA policy. Specifically, NCUA identified [redacted] had not remediated them. Examples include:

- [redacted] on the server to instruct a browser to only [redacted]
- [redacted] including information disclosure vulnerabilities [redacted]
- [redacted] by someone observing network traffic to the effected device, and;
- [redacted] may aid an attacker to determine information and configurations [redacted]

[redacted]

Office of the Chief Information Officer (OCIO) management indicated:

- Software vulnerabilities were present on the network because OCIO focused on remediating higher risk vulnerabilities [redacted]
- NCUA has been in the process of migrating [redacted] platforms. However, this process was still ongoing during FY 2020.

OCIO management also specified that NCUA has compensating controls in place, including firewalls, intrusion detection systems, endpoint protection and vulnerability surveillance to provide enhanced monitoring and detection of suspected malicious activity. CLA validated these compensating controls were in place.

NIST SP 800-53, Revision 4, security control System and Information Integrity (SI)-2, Flaw Remediation, requires organizations to install security-relevant software and firmware updates within an organization-defined time period of the release of the updates.

In addition, OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, 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.

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.
- 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.

By timely installing required patches, 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[17] 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

[17] Ibid 7.

to supported platforms before support for the software ends. Although we acknowledge NCUA has implemented a process to detect unsupported software, NCUA had not migrated the unsupported software to supported platforms, and did not meet agency defined timeframes for remediation of moderate 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 Ensure System Accounts for Separated Personnel are Disabled

FY 2020 IG FISMA Metric Area: *Identity and Access Management*

NCUA did not effectively disable remote access and network accounts of separated employees and contractors. Specifically, we reviewed remote access and network accounts and determined that NCUA did not timely disable the accounts for one of 47 separated employees and two of 54 separated contractors in accordance with NCUA policy. NCUA policy requires disabling of user access within four hours after the close of business on the last day of employment with the NCUA. NCUA disabled these accounts between four days and five months after the users separated from NCUA.

Management stated that the accounts were not disabled timely for the separated employees and contractors because the Employee Exit Form workflow was not initiated and completed in SharePoint within the required timeframe. The Employee Exit Form is the means by which NCUA personnel provide notification of an employee or contractor separation via a workflow process in SharePoint. NCUA uses an automated script to remove separated users' network access daily in accordance with the separation date on the Employee Exit Form.

NIST SP 800-53, Revision 4, security control Personnel Security (PS)-4, Personnel Termination, requires that upon terminating employment, organizations will disable information system access and notify *organization-defined personnel or roles* within an *organization-defined time period*.

The *NCUA Information Security Procedural Manual* control AC-2f requires termination/disabling of employee access within four hours after the close of business on the last day of employment with the NCUA. Additionally:

- Control PS-4f requires that NCUA personnel (direct supervisor/manager, Office of Continuity and Security Management, and/or Office of Human Resources) be notified within seven calendar days of the individual's termination.

- Control PS-4a requires that information system access be terminated/disabled as soon as possible but no longer than seven calendar days following termination or, if necessary, prior to the formal termination action.

We determined there is an inconsistency in the agency's controls as stipulated in the *NCUA Information Security Procedural Manual.* Specifically, while the AC-2f control requires NCUA to disable the separated users' information system access within four hours after close of business on the last day of the users' employment, the PS-4 control allows NCUA personnel up to seven days to provide the separation notification.

Effective management of user accounts will help NCUA guard against unauthorized access to the agency's information, decreasing the likelihood of improper modification, loss, and unauthorized disclosure of personally identifiable information and sensitive agency data. If NCUA account management policies contradict, NCUA personnel may be confused about management's desired intent for control implementation.

To assist the NCUA in strengthening account management controls for separated employees and contractors, we recommend that NCUA management:

FY2020 Recommendation 1: *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.*

Agency Response:
By December 31, 2021, management will review 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 document the timeframe in the NCUA Information Security Procedural Manual.

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

FY2020 Recommendation 2: *Develops and implements a monitoring process to ensure the Employee Exit Form process is completed in accordance with the timelines established in NCUA policy.*

Agency Response:
By December 31, 2021, management will implement a monitoring process to ensure the Employee Exit Form process is completed in accordance with policy.

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

4. The NCUA Needs to Ensure All Network Users Complete Access Agreements

FY 2020 IG FISMA Metric Area: *Identity and Access Management*

NCUA did not ensure all network users agreed to the NCUA's security and privacy rules for using its network and accessing agency information (NCUA Rules of Behavior) prior to or since the agency authorized the users to access its network. Specifically, we sampled 18 network users and noted that one employee and one contractor did not sign the required NCUA Rules of Behavior agreement. They have been accessing the NCUA's network and information for more than six months without having signed the agreement.

Management stated that during new employee orientation, employees are directed to complete the information security awareness training and sign the Rules of Behavior via SharePoint before receiving their laptop. According to management, one of the new users onboarded remotely and the other individual onboarded in person at NCUA Headquarters. For either method of onboarding, management stated there is not an enforcement mechanism in place to ensure the Rules of Behavior are signed. Additionally, management indicated enforcement is more of a challenge for remote onboarding because in its electronic form, the Rules of Behavior is only available on the agency's intranet (SharePoint site) or during online security awareness training after a user has received their laptop and has access to the agency's network.

NIST SP 800-53, Revision 4, security control Personnel Security (PS)-6, Access Agreements, requires organizations to ensure that all individuals requiring access to organizational information and information systems sign appropriate access agreements (rules of behavior) prior to being granted access indicating that they have read, understand, and agree to abide by the rules of behavior. The access agreements describe their responsibilities and expected behavior with regard to information and information system usage.

The NCUA *General Support System (GSS) System Security Plan* stipulates:

- NCUA employs appropriate access agreements (e.g., rules of behavior, etc.) to be signed by individuals requiring access to OCIO information and information systems prior to being granted access.

- All individuals responsible for the management, operation and maintenance of the information system and components or devices that support the information system are required to provide acknowledgment indicating that they have read, understand and agree to abide by the Rules of Behavior. The Rules of Behavior attestation of compliance is presented to the user upon initial login into the NCUA's network, when the user account is first authorized as part of the onboarding process and annually as part of the general security awareness training.

By ensuring its users acknowledge the agency's rules for accessing its network and its information prior to allowing the users to access its network, NCUA will ensure its users are aware of their privacy and security responsibilities, helping to increase the security of the agency's network and maintain the privacy of confidential and sensitive information.

The FY 2019 FISMA Audit Report included a recommendation[18] to ensure the CIO develops and implements a process to document and maintain evidence that users sign access agreements prior to accessing the agency's network. Management communicated that corrective action was completed for this recommendation. However, since we found the same issue again this year, the recommendation will remain open; therefore we are not making a new recommendation.

[18] Ibid 10.

Appendix I

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,[19] 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 19, 2019, OMB issued Memorandum M-20-04, *Fiscal Year 2019-2020 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 2020 IG FISMA Reporting Metrics, provided reporting

[19] 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.[20]

The FY 2020 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 2020 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	Domains in the FY 2020 IG FISMA Reporting Metrics
Identify	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 2020 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.

[20] https://www.cisa.gov/publication/fy20-fisma-documents

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this performance audit was to assist the NCUA OIG in assessing the NCUA's compliance with FISMA and agency information security and privacy policies and procedures.

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

The scope of the audit included assessing select NIST 800-53, Revision 4, security and privacy controls mapped to the following FY 2020 IG FISMA Reporting Metrics domains for four NCUA information systems:

- 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 39 information system in the NCUA's system inventory:

- General Support System (GSS)
- Credit Union Online (CUOnline)
- Insurance Information System (IIS)
- Credit Union Service Organization Registry (CUSO Registry)

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.[21] Audit fieldwork covered NCUA's headquarters located in Alexandria, VA, from June 10 to October 20, 2020. The scope of the audit covered the period from October 1, 2019, through September 30, 2020.

Methodology

To determine if the NCUA implemented an effective information security program, CLA conducted interviews with NCUA officials and reviewed legal and regulatory requirements stipulated in FISMA. Also, CLA 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, CLA compared documents, such as the NCUA's information technology policies and procedures, to requirements stipulated in NIST special publications. In addition, CLA 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 2020 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 for the adequacy and effectiveness of the security controls, CLA exercised professional judgment in determining the number of items selected for testing and the method used to select them. Relative risk and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review was considered. 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.

[21] *FY 2019 National Credit Union Administration's Federal Information Security Modernization Act of 2014 Audit*, (OIG Report No. OIG-19-10, December 12, 2019).

Appendix III

STATUS OF PRIOR YEAR RECOMMENDATIONS

The table below summarizes the status of our follow up related to the prior recommendations reported for the FY 2019 FISMA audit.[22] During FY 2020, the NCUA implemented corrective actions to close twelve prior year recommendations from the FY 2019 FISMA audit report.

Recommendation	Status Determined by NCUA	Auditor Position on Status of Recommendation
2018-2: The NCUA management ensure system owners for the GSS (the Office of the Chief Information Officer) and the IIS (Credit Union Resources and Expansion) address all control weaknesses from Security Control Assessments in their System Risk Assessments and Plans of Action and Milestones.	Closed	Closed
2018-3: The NCUA management ensure the system owners timely and adequately manage and maintain the completion dates within the Plan of Action and Milestones.	Closed	Closed
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, this issue was 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.	Closed	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.	Closed	Open See finding 2
2018-10: The Office of the Chief Information Officer implement a process to identify authorized software in its	Open	Open

[22] Ibid 21.

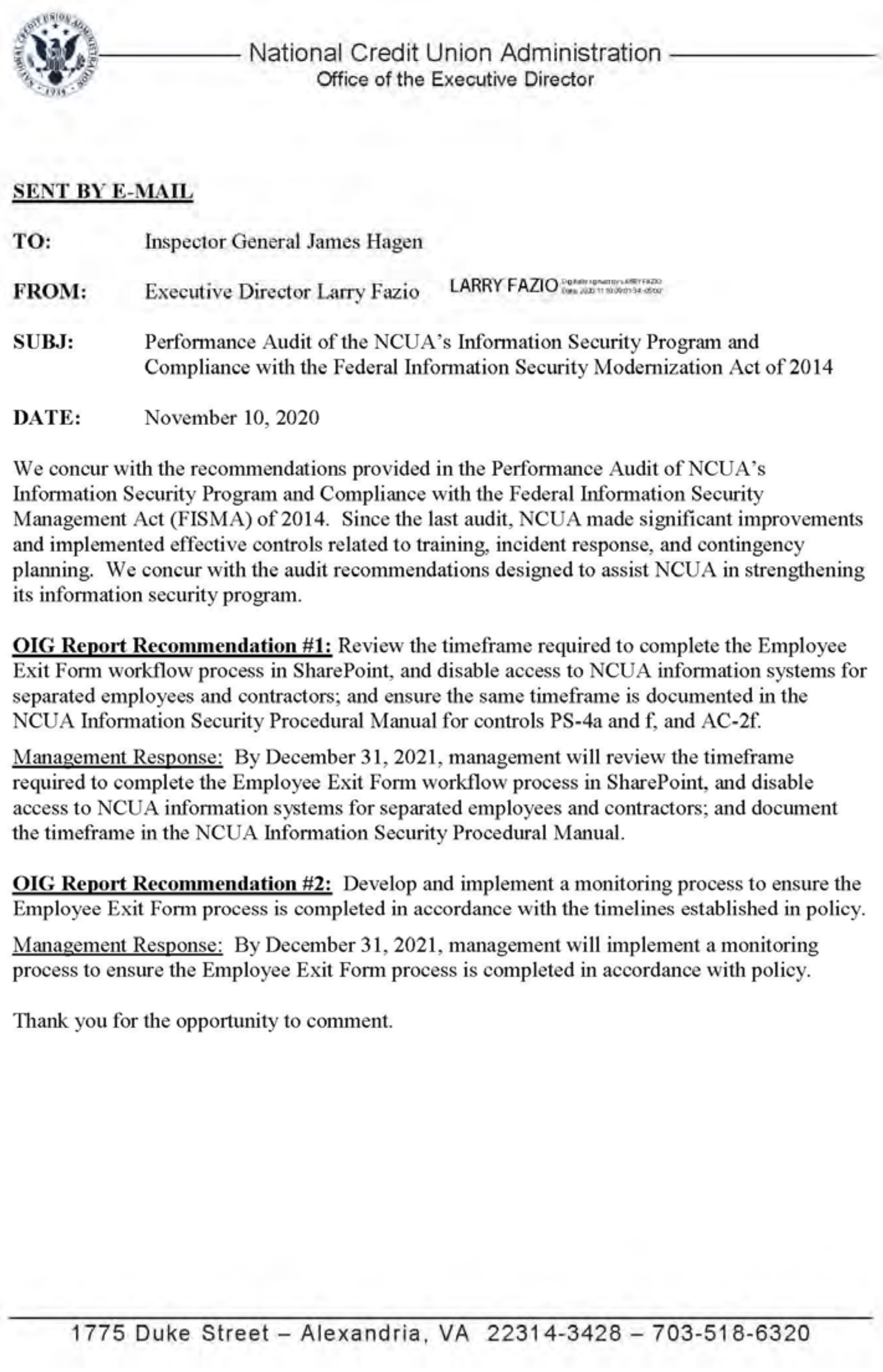
Recommendation	Status Determined by NCUA	Auditor Position on Status of Recommendation
environment and remove any unauthorized software.		Based on the corrective action plan provided by NCUA management, this issue was not scheduled for completion until November 30, 2020.
2019-1: The NCUA management ensures the Agency addresses all control weaknesses documented in the system security plans and security assessment reports in their Plan of Action and Milestones. (Repeat)	Closed	Closed
2019-2: The NCUA management ensures the Agency timely and adequately manages and maintains the completion dates within the Plan of Action and Milestones. (Repeat)	Closed	Closed
2019-3: The NCUA management ensures the Agency performs likelihood analysis on all known vulnerabilities from all sources as part of its information system risk assessment.	Open	Open Based on the corrective action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2020.
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, this issue was 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.	Open	Open Based on the corrective action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2020.
2019-6: The NCUA management ensures the Agency completes and documents a security impact analysis for	Open	Open

Recommendation	Status Determined by NCUA	Auditor Position on Status of Recommendation
emergency changes in accordance with the OCIO Operational Change Control Board Charter.		Based on the corrective action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2020.
2019-7: The NCUA management ensures the CUSO Registry system owner obtain a risk acceptance from the Authorizing Official for the deviation from NCUA policy for inactive accounts.	Closed	Closed
2019-8: The NCUA management ensures the CUOnline and CUSO Registry system owner restrict access to non-public data to only those users who require it, in accordance with the concept of least privilege.	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	Open See finding 4
2019-10: The NCUA management ensures the Senior Agency Official for Privacy develops and implements a formal Privacy Continuous Monitoring Strategy that includes a formal process for assessing agency privacy controls on at least an annual basis as required by OMB.	Closed	Closed
2019-11: The NCUA management ensures the Senior Agency Official for Privacy develops and implements a process to identify and review metrics to measure the effectiveness of privacy activities and compliance with privacy requirements as specified by OMB.	Closed	Closed
2019-12: The NCUA management ensures the Senior Agency Official for Privacy develops and implement a process to review and update privacy-related policies and procedures on at least a biennial basis in accordance with NIST SP 800-53, Revision 4.	Closed	Closed

Recommendation	Status Determined by NCUA	Auditor Position on Status of Recommendation
2019-13: The NCUA management appoints an authorizing official that is in line with NIST 800-37, Risk Management Framework for Information Systems and Organizations, Revision 2.	Closed	Closed
2019-14: The NCUA management ensures the new authorizing official completes the process of reauthorizing all of the NCUA's information systems by signing new authorization decision documents.	Closed	Closed
2019-15: The NCUA management ensures annual independent security control assessments are conducted for all agency information systems.	Closed	Closed

Appendix IV

MANAGEMENT COMMENTS



National Credit Union Administration
Office of the Executive Director

SENT BY E-MAIL

TO: Inspector General James Hagen

FROM: Executive Director Larry Fazio LARRY FAZIO Digitally signed by LARRY FAZIO Date: 2020.11.10 09:01:34 -05'00'

SUBJ: Performance Audit of the NCUA's Information Security Program and Compliance with the Federal Information Security Modernization Act of 2014

DATE: November 10, 2020

We concur with the recommendations provided in the Performance Audit of NCUA's Information Security Program and Compliance with the Federal Information Security Management Act (FISMA) of 2014. Since the last audit, NCUA made significant improvements and implemented effective controls related to training, incident response, and contingency planning. We concur with the audit recommendations designed to assist NCUA in strengthening its information security program.

OIG Report Recommendation #1: Review 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.

Management Response: By December 31, 2021, management will review 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 document the timeframe in the NCUA Information Security Procedural Manual.

OIG Report Recommendation #2: Develop and implement a monitoring process to ensure the Employee Exit Form process is completed in accordance with the timelines established in policy.

Management Response: By December 31, 2021, management will implement a monitoring process to ensure the Employee Exit Form process is completed in accordance with policy.

Thank you for the opportunity to comment.

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320