NCUA
National Credit Union Administration

OFFICE OF INSPECTOR GENERAL

NATIONAL CREDIT UNION ADMINISTRATION FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014 AUDIT—FISCAL YEAR 2019

Report #OIG-19-10
December 12, 2019

Office of Inspector General

SENT BY EMAIL

TO: Distribution List

FROM: Inspector General James W. Hage

SUBJ: National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit—Fiscal Year 2019

DATE: December 12, 2019

Attached is Office of the Inspector General's FY 2019 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 15 recommendations that will assist the agency in improving the effectiveness of its information security and its privacy programs and practices. NCUA management concurred with all of the recommendations and is continuing its efforts or 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 Mark Treichel
Acting General Counsel Frank Kressman
Deputy Executive Director John Kutchey
Spec Asst. to the ED Joy Lee
Deputy Chief of Staff Gisele Roget
OEAC Deputy Director Michael Sinacore
Chief Information Officer Robert Foster
Chief Financial Officer Rendell Jones
AMAC President Keith Morton
E&I Director Larry Fazio
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

National Credit Union Administration

Federal Information Security Modernization Act of 2014 Audit

Fiscal Year 2019

Final Report

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

December 9, 2019

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 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 2019.

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 2019 in accordance with the Federal Information Security Modernization Act of 2014 (FISMA). 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 the 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.

Our audit was performed 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.

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 6 of 33 systems in the NCUA's inventory of information systems. The security controls selected for testing were mapped to the Department of Homeland Security's IG FISMA metrics for assessing the maturity of an agency's information security program in eight IG FISMA Metric Domains and five Function Areas. Audit fieldwork was performed at the NCUA's headquarters in Alexandria, VA from June 12, 2019 to September 30, 2019.

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. We identified weaknesses in five of the eight domains of the FY 2019 IG FISMA Reporting Metrics related to risk management, configuration management, identity and access management, data protection and privacy, and information security continuous monitoring. 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 15 recommendations to assist the NCUA in strengthening its information security program. In addition, our review of the prior FISMA recommendations determined that 6 of the 11 OIG prior year 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 current status. We concluded our fieldwork and assessment on September 30, 2019. We have no obligation to update our report or to revise the information contained therein to reflect events occurring subsequent to September 30, 2019.

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

Arlington, Virginia
December 9, 2019

NATIONAL CREDIT UNION ADMINISTRATION
FY 2019 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) 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 October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 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 FY 2019 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 1.0: Identify, Protect, Detect, Respond, and Recover, as highlighted in **Table 1**. The IG FISMA Metrics consists of 67 objective questions divided into eight domains, which correspond to the five security functions. 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 assessment grades maturity on a scale from Level 1 (Ad hoc) to Level 5 (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 2019 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*.

Table 1: Alignment of the Cybersecurity Framework Security Functions to the Domains in the FY 2019 IG FISMA Reporting Metrics

Cybersecurity Framework Security Functions	Domains in the FY 2019 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

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 6 of 33 information systems in the NCUA's information system inventory as of June 12, 2019. 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 six NCUA information systems that we tested.

The audit was performed in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for the findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the 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 2**. 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.

Table 2: Calculated Maturity Ratings by Function Area, Domain and Overall

Security Function	Calculated Maturity Level by Function FY 2019	IG FISMA Metric Domains	Calculated Maturity Level by Domain FY 2019
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)

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

Security Function	Calculated Maturity Level by Function FY 2019	IG FISMA Metric Domains	Calculated Maturity Level by Domain FY 2019
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	**Not Effective**		

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 2019 FISMA audit. Although we identified areas for improvement this year, we deemed the NCUA's overall information security program effective. 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.

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 five of the eight domains of the FY 2019 IG FISMA Reporting Metrics related to risk management, configuration management, identity and access management, data protection and privacy, and information security continuous monitoring (see **Table 3**). 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.

We have made 15 recommendations to assist the NCUA in strengthening its information security program. In addition, our review of the prior FISMA recommendations determined that 6 of the 11 OIG prior year open recommendations related to the NCUA's security program and practices remain open. Refer to Appendix III for a detailed description of the status of each recommendation.

Table 3: Weaknesses Noted in FY 2019 FISMA Independent Evaluation Mapped to Cybersecurity Framework Security Functions and Domains in the FY 2019 IG FISMA Reporting Metrics

Cybersecurity Framework Security Function	FY 2019 IG FISMA Reporting Metrics Domain	Weaknesses Noted
Identify	**Risk Management**	The NCUA did not create Plan of Action and Milestones (POA&Ms) for all known information security control weaknesses, and did not adequately manage POA&M completion dates. **(Finding 1)**

Cybersecurity Framework Security Function	FY 2019 IG FISMA Reporting Metrics Domain	Weaknesses Noted
		The NCUA did not document and analyze all known control weaknesses in information system risk assessments. **(Finding 1)**
Protect	**Configuration Management**	The NCUA did not implement [redacted] in accordance with NIST requirements and NCUA policy. **(Finding 2)**
		The NCUA did not consistently implement information system changes in accordance with NCUA policy. **(Finding 2)**
	Identity and Access Management	The NCUA did not consistently implement account management controls. **(Finding 3)**
	Data Protection and Privacy	The NCUA did not test and evaluate the effectiveness of privacy policies, procedures, and practices on at least an annual basis as required by OMB. **(Finding 4)**
		The NCUA did not consistently update privacy-related policies and procedures at least biennially as required by NIST. **(Finding 4)**
	Security Training	No weaknesses noted.
Detect	**Information Security Continuous Monitoring**	The NCUA did not maintain its security authorization process in accordance with NIST requirements. **(Finding 5)**
		The NCUA did not conduct an annual security control assessment in accordance with NCUA policy. **(Finding 6)**
Respond	**Incident Response**	No weaknesses noted.
Recover	**Contingency Planning**	No weaknesses noted.

In response to the draft report, the NCUA concurred with all 15 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 comments are included in their entirety in Appendix IV.

The following section provides a detailed discussion of the audit findings. Appendix II describes the audit objective, scope and methodology.

FISMA Audit Findings

Security Function: Identify

1. The NCUA Needs to Improve its Risk Management Process

FY 2019 IG FISMA Metric Area: *Risk Management*

The NCUA did not effectively manage some elements of its POA&Ms and information system risk assessments.

Plan of Action and Milestones

- The NCUA system owners did not create POA&Ms for all known information security control weaknesses for the General Support System (GSS), Call Report System (CUOnline), Credit Union Service Organization Registry (CUSO Registry), and the Asset Liquidation Management System (ALMS). Specifically, the NCUA did not create POA&Ms for the following known control weaknesses:
    - GSS
        - 24 controls designated as not implemented in the System Security Plan (SSP).
        - 7 controls recorded as not satisfied in 2018 Security Controls Assessment (SCA).
    - CUOnline
        - 39 controls designated as not implemented in the SSP.
    - CUSO Registry
        - 11 controls designated as not implemented in the SSP.
    - ALMS
        - 5 controls designated as not implemented in the SSP.
- The NCUA system owners did not adequately manage POA&M completion dates. Specifically, the system owners for the following systems did not meet the scheduled completion dates, and did not document new completion dates for the number of POA&Ms as indicated:
    - GSS – 23 POA&Ms
    - Automated Integrated Regulatory Examination System (AIRES) - 2 POA&Ms

Although the NCUA has made progress since last year's audit, work still remains for the NCUA to improve the management of the POA&M process. NCUA management stated they did not consistently ensure POA&Ms were created for all control weaknesses and did not properly manage POA&M completion dates due to lack of sufficient oversight.

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to develop and maintain a plan of action and milestones for the information system to document the organization's planned remedial actions to correct weaknesses or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and update existing plan of action and milestones based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

In addition, the *NCUA Information Security Procedural Manual,* requires the following:

- Developing POA&Ms to document the planned remedial actions to correct weaknesses or deficiencies noted during the SCA and to reduce or eliminate known vulnerabilities in the system. Requests for extending the scheduled completion date with a justification for the extension is required, in writing, to the CISO who reviews and approves or rejects extensions based on risk to the agency and the provided justification. The system owner and Information System Security Officer (ISSO) are responsible for creating and maintaining POA&Ms.

Risk Assessments

- The NCUA did not address all known vulnerabilities (control weaknesses) in the GSS, CUOnline, CUSO Registry, and ALMS information system risk assessments. Specifically, information system risk assessments did not include the following known control weaknesses:

    - GSS
        - 24 controls designated as not implemented in the SSP.
        - 7 controls recorded as not satisfied in the most recent SCA.
        - 22 control weaknesses listed as open POA&Ms.
    - CUOnline
        - 39 controls designated as not implemented in the SSP.
    - CUSO Registry
        - 11 controls designated as not implemented in the SSP.
    - ALMS
        - 5 controls designated as not implemented in the SSP.
        - 2 control weaknesses listed as open POA&Ms.

    Office of the Chief Information Officer (OCIO) management informed us they exercised their discretion concerning the content and level of detail to include in the risk assessments and made a decision to exclude the vulnerability identification from the risk assessments.

- The NCUA did not consistently perform analysis of the likelihood that threat events could exploit the control weaknesses. Although the NCUA performed likelihood analysis for control weaknesses noted in SCAs, the NCUA did not perform likelihood analysis of control weaknesses that were reported via Inspector General audits, which represents

approximately 20% of the NCUA's control weaknesses for the systems selected for testing. While the NCUA has been performing its likelihood analysis determinations within the SCAs reports, management indicated there was not a process in place to perform likelihood analysis on vulnerabilities identified from other sources.

NIST SP 800-53, Revision 4, requires organizations to conduct an assessment of risk,[5] including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits.[6]

NIST SP 800-30 Rev 1, *Guide for Conducting Risk Assessments* (September 2012), indicates that in conducting risk assessments, organizations:

- Determine which types of threat sources, threat events, and vulnerabilities are to be considered during risk assessments; and
- Make explicit the process used to conduct likelihood determinations and impact determinations and any assumptions related to the likelihood and impact determination processes.

NIST 800-30 also indicates that potential inputs to its process of determining its vulnerabilities at the information system level (Tier 3),[7] include (but are not limited to):

- Vulnerability information and guidance specific to Tier 3 (e.g., vulnerabilities related to information systems, information technologies, information system components, applications, networks, environments of operation).
- Security assessment reports (i.e., deficiencies in assessed controls identified as vulnerabilities).
- Results of monitoring activities (e.g., automated and non-automated data feeds).
- Vulnerability assessments, Red Team reports, or other reports from analyses of information systems, subsystems, information technology products, devices, networks, or applications.
- Contingency Plans, Disaster Recovery Plans, Incident Reports.
- Vendor/manufacturer vulnerability reports.

[5] NIST and OMB define risk as: "A measure of the extent to which an entity is threatened by a potential circumstance or event, and typically a function of: (i) the adverse impacts that would arise if the circumstance or event occurs; and (ii) the likelihood of occurrence."

[6] NIST describes a risk assessment as: "The process of identifying risks to organizational operations (including mission, functions, image, reputation), organizational assets, individuals, other organizations, and the Nation, resulting from the operation of an information system. Part of risk management, incorporates threat and vulnerability analyses, and considers mitigations provided by security controls planned or in place."

[7] NIST Special Publication 800-39, Revision 1, *Managing Information Security Risk Organization, Mission, and Information System View*, specifies an integrated risk management process three-tiered approach for managing risk across an organization that "addresses risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization."

In addition, the *NCUA Information Security Procedural Manual,* requires conducting a risk assessment in accordance with NIST. The ISSO is responsible for the risk assessment.

By conducting analysis of information system vulnerabilities and the likelihood that threat sources could exploit a vulnerability, the NCUA will be able to determine the severity of the risks, and the prioritization of remediation activities. In addition, by adequately managing and documenting risk assessments and POA&Ms under the continuous monitoring process, the authorizing official will have sufficient and appropriate information (1) regarding known security vulnerabilities and any applicable privacy or security risks; (2) the mitigation of known privacy or security control weaknesses; and (3) the estimated timeline to remediate any system privacy or security weaknesses. Ultimately, the NCUA will be able to more effectively maintain the security posture of the NCUA information systems at an acceptable level of risk, mitigating the potential compromise of the confidentiality, integrity and availability of the NCUA's information and information systems.

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

Recommendation 1: *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)*

Agency Response:
Management concurred with the recommendation. Management indicated that by December 31, 2020, the NCUA will implement a quality assurance review to improve system security documentation, including identifying control weaknesses and establishing POA&Ms resulting from security controls assessments.

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

Recommendation 2: *Ensures the Agency timely and adequately manages and maintains the completion dates within the Plan of Action and Milestones. (Repeat)*

Agency Response:
Management concurred with the recommendation. Management indicated that by December 31, 2020, the NCUA will implement a quality assurance review to manage POA&M completion dates in accordance with NCUA policy.

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

Recommendation 3: *Ensures the Agency performs likelihood analysis on all known vulnerabilities from all sources as part of its information system risk assessment.*

Agency Response:
Management concurred with the recommendation. Management indicated that by December 31, 2020, the NCUA will implement a quality assurance review to review and update the assessment and authorization procedures to ensure the likelihood analyses are consistently performed and documented in the information system risk assessment.

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

Security Function: Protect

2. The NCUA Needs to Improve its Configuration Management Controls

FY 2019 IG FISMA Metric Area: *Configuration Management*

We noted control weaknesses with the NCUA's configuration management controls in the following areas:

- [redacted]
- System Change Controls

[redacted]
The NCUA did not implement [redacted] in accordance with NIST requirements and NCUA policy. For example, we noted the NCUA:

- Did not implement [redacted].
- Did not fully implement [redacted] and did not implement them at all [redacted]:
  - [redacted]

OCIO management informed us that they implemented a freeze on configuration changes from March 2018 to April 2019 while rolling out [redacted] on the NCUA [redacted]. Management also stated that they delayed implementing DISA STIG configuration settings on [redacted] because the agency was migrating from [redacted] that began in May 2019. Management stated they expect to begin applying baselines to [redacted] in 2020, with an estimated completion date of 2024.

OCIO management also indicated that modernizing the CUSO Registry, CUOnline, AIRES and Insurance Information System (IIS) legacy applications must be completed prior to applying [redacted] that support them. Applying [redacted] would increase the risk of those applications not functioning properly. Management informed us the Modern Examination and Risk Identification Tool (MERIT), the AIRES replacement, is currently in testing and will be rolled out this calendar year. In addition, management informed us the NCUA has initiated the requirements gathering for the updated IIS; but has not determined the scheduled decommission date for the current legacy version. Management has also not determined the scheduled decommission date for the legacy CUOnline and CUSO Registry systems.

[8] The NCUA is in the process of building out a new SharePoint environment in which [redacted] will be applied.

NIST SP 800-53, Revision 4, requires agencies to document and implement configuration settings for their information technology, document and approve any deviations from the configuration settings, and monitor for compliance with the approved configuration settings.

The *NCUA Information Security Procedural Manual* states:

- "Establish and document configuration settings for information technology products employed within the information system using NCUA-defined security configuration checklists that reflect the most restrictive mode consistent with operational requirements. NCUA-defined security configuration checklists include Defense Information Systems Agency Security Technical Implementation Guides and United States Government Configuration Baseline."

Implementing and monitoring [redacted] helps ensure that system configurations are secure, decreasing the risk of either intentional or inadvertent altering from the [redacted] without management's knowledge. Ultimately, this helps ensure the confidentiality, integrity and availability of agency systems, personally identifiable information and sensitive data.

System Change Controls

The NCUA did not implement information system changes in accordance with NCUA policy. Specifically,

- The NCUA implemented two out of 21 sampled normal changes to the GSS, one out of two sampled changes to AIRES, and one out of two sampled changes to IIS without the Change Control Board (CCB) reviewing the test results.
- The NCUA did not complete the Security Impact Analysis (SIA) during post implementation review for three out of 21 sampled emergency GSS changes.

We validated that test results were documented for one of the GSS sampled system changes and all of the ARIES and ISS sampled system changes. However the documentation was not included in ServiceNow (the change management ticketing system) for the CCB to review. OCIO management informed us that the test results were not uploaded in ServiceNow for review due to an oversight. In addition, OCIO management informed us the SIA was also not completed for the emergency changes during the post implementation review due to an oversight.

NIST SP 800-53, Revision 4, requires agencies to test system changes and analyze the changes to determine potential security impacts, prior to implementing the changes into the operational environment.

The *NCUA Information Security Procedural Manual* states, "test, validate, and document changes to the information system before implementing the changes on the operational system."

The NCUA's *General Support System Configuration Management Plan*, version 2.0 states:

- "A normal change must go through the full change management process before being approved and implemented.

- The configuration change control process for the information system must include a systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications."

The NCUA's *OCIO Operational Change Control Board Charter* states, "All changes are analyzed and evaluated for adverse impact on security, preferably before they are approved and implemented, but also in the case of emergency/unscheduled changes. For emergency/unscheduled changes, the security impact analysis will be part of the post implementation review."

Ensuring that the CCB reviews the test results for all information system changes helps ensure that the changes will not cause functionality issues for end users and adversely impact the operation of agency systems. Furthermore, by documenting the detailed analysis of the security impact of changes on NCUA systems, the NCUA can advance its efforts in developing and maintaining the secure state of its information systems and mitigate exposure of its systems to potential threats and attacks.

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

Recommendation 4: *Ensures the Agency implements, tests, and monitors [redacted] in the NCUA information technology environment in compliance with established NCUA security standards. This includes documenting approved deviations from [redacted] with business justifications.*

Agency Response:
Management concurred with the recommendation. Management indicated that by December 31, 2024, the NCUA will implement, test, and monitor [redacted] in the NCUA information technology environment in compliance with established NCUA security standards.

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

Recommendation 5: *Ensures the Agency maintains and reviews test results in ServiceNow for all system changes.*

Agency Response:
Management concurred with the recommendation. Management indicated that by December 31, 2020, the NCUA will implement a quality review process to ensure test results are maintained and reviewed for all system changes.

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

Recommendation 6: *Ensures the Agency completes and documents a security impact analysis for emergency changes in accordance with the OCIO Operational Change Control Board Charter.*

Agency Response:
Management concurred with the recommendation. Management indicated that by December 31, 2020, the NCUA will update policies and procedures to ensure security impact analysis results are incorporated into its change process for emergency changes.

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

3. The NCUA Needs to Strengthen its Account Management Controls

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

We noted weaknesses with the NCUA's account management controls in the following areas:

- Inactive Accounts
- Least Privilege Access
- User Access Agreements

Inactive Accounts
CUSO Registry is not configured to disable inactive accounts in accordance with the NCUA policy. 483 from the total population of 2,248 accounts [redacted]

NCUA management informed us the system owner, in consultation with the NCUA CISO, agreed [redacted] because the system is used once a year by external users. NCUA management also stated that the system owner documented the deviation from NCUA policy in the CUSO Registry's SSP in 2017, 2018, and 2019 and the system was authorized by the Authorizing Official (AO) in 2017, and again in 2018. The system owner did not request a risk acceptance from the AO because the deviation from policy was agreed to by the CISO and the system owner interpreted the agreement as approval. Additionally, NCUA management informed us that the internal user's network accounts [redacted], as a compensating control.

NIST 800-53 Rev 4 requires agency information systems to automatically disable inactive accounts after a period of time as set by the agency. The *NCUA Information Security Procedural Manual* requires inactive accounts to be automatically [redacted].

Properly managing inactive user accounts will help the agency decrease the risk of unauthorized or improper access to Personally Identifiable Information (PII) or sensitive agency data.

Least Privilege Access
The NCUA did not fully apply the principle of least privilege to CUOnline and CUSO Registry user accounts. NCUA employees [redacted] to both the public and non-public data in CUOnline and CUSO Registry. 283 from the total population of 1,268 CUOnline and 73 from the total population of 2,248 CUSO Registry active users [redacted] to the respective

systems. Some of these CUOnline accounts and CUSO Registry accounts were created as far back as 2012 and 2017[9] respectively.

NCUA management informed us that the NCUA Board made a decision in 2009 [redacted] to the online profile and call report system. NCUA management also informed us that some system users may not need access to non-public data to perform their job duties because the data collected from the systems is available in reports, therefore users do not need to log into the system to see entity level data.

NIST 800-53 Rev 4 requires the agency to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions. The *NCUA Information Security Procedural Manual* requires employment of the principle of least privilege, allowing only authorized accesses for users which are necessary to accomplish assigned tasks.

Employing the principle of least privilege access limits the number of users with access to sensitive information, thereby decreasing the risk of unauthorized modification, loss, and disclosure of PII or sensitive agency data.

User Access Agreements

The NCUA did not provide evidence to validate that nine out of a sample of 25 new network users tested (36 percent), signed an access agreement *prior to* gaining access to the NCUA network. Specifically, the NCUA was not able to provide a system generated report detailing first logon date or any other viable evidence showing the users signed the access agreements prior to logging on to the network. The evidence provided showed the users signed access agreements after their start dates and account create dates.

NIST 800-53 Rev 4 requires the agency to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access. The *NCUA Information Security Procedural Manual* stipulates that individuals requiring access to NCUA information and information systems must sign access agreements prior to being granted access.

User access agreements formally document that the NCUA has apprised users of the limitations and rules associated with using its information systems and the users' agreement to abide by these limitations and rules. As a result, the NCUA will have greater assurance that system users are aware of their responsibilities when using the agency's information systems, helping to increase the security of the agency's data.

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

> ***Recommendation 7****: Ensures the CUSO Registry system owner obtain a risk acceptance from the Authorizing Official for the deviation from NCUA policy for inactive accounts.*

[9] The CUSO Registry system went live on February 1, 2016.

Agency Response:
Management concurred with the recommendation. Management indicated that by June 30, 2020, the NCUA will ensure the CUSO Registry system owner obtains a risk acceptance from the Authorizing Official for the deviation from NCUA policy for inactive accounts.

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

Recommendation 8*: 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.*

Agency Response:
Management concurred with the recommendation. Management indicated that by June 30, 2020, the CU Online and CUSO Registry system owners will obtain a risk acceptance from the Authorizing Official for the deviation from NCUA policy for least privilege access.

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

Recommendation 9*: 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.*

Agency Response:
Management concurred with the recommendation. Management indicated that by June 30, 2020, the NCUA will update the information security policy and procedures to ensure that signed information system access agreements are documented and maintained.

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

4. The NCUA Needs to Strengthen its Privacy Monitoring Program

FY 2019 IG FISMA Metric Area: *Data Protection and Privacy*

We noted issues with monitoring and auditing of privacy controls, and the review and update to privacy-related policies and procedures.

Privacy Monitoring and Auditing
The NCUA did not test and evaluate the effectiveness of privacy policies, procedures, and practices on at least an annual basis as required by OMB. Although a selection of privacy controls were listed in the SCA plans for the information systems we reviewed, the agency did not test them within the last year. In addition, the NCUA did not identify metrics, which would enable the agency to determine whether its privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements.

The NCUA Senior Agency Official for Privacy (SAOP) stated the privacy office relies on the annual FISMA audit for this and had not formally developed a Privacy Continuous Monitoring (PCM) strategy. However, privacy continuous monitoring is intended to be a program designed and implemented by the agency's privacy office to assess and measure the effectiveness of its privacy policies, procedures and practices. The FISMA audit is a high level review of the privacy program and assesses only a select number of privacy controls.

OMB Circular A-130, *Managing Information as a Strategic Resource*, Appendix II, Section I Risk Management Framework, requires that the SAOP develops and maintains a PCM strategy and PCM program to maintain ongoing awareness of privacy risks. This includes conducting privacy control assessments, and identifying metrics to determine whether privacy controls are implemented correctly, operating as intended, and sufficient to ensure compliance with applicable privacy requirements and manages privacy risks. Agencies must ensure that periodic testing and evaluation of the effectiveness of information security and privacy policies, procedures, and practices are performed with a frequency depending on risk, but at least annually.

By periodically assessing the agency's privacy controls, the NCUA will be able to determine the extent to which the controls are operating effectively or as intended, are sufficient to ensure compliance with applicable privacy requirements, and are producing the desired outcome. As a result, the NCUA will be more aware of privacy program risks and the potential for agency and credit union staff mismanaging PII.

Privacy Policies and Procedures

Although the NCUA updated the *NCUA Privacy Program Plan* in 2018, the agency did not update the following privacy-related policies and procedures at least biennially as required by NIST:

- NCUA Instruction NO. 3226.1 (Rev. 1), *Privacy Act of 1974 (PA) Compliance*, June 25, 2008
- NCUA Instruction NO. 13500.08 (Rev. 1), *Breach Reporting and Notification Policy*, August 27, 2015
- NCUA Instruction NO. 13500.09 (Rev. 1), *Security of Sensitive Information*, August 27, 2015
- *SORN Guidance*, November 2016

The NCUA SAOP stated the *NCUA Privacy Program Plan* is the agency's overarching document for its privacy program with related Instructions and Guidance. The SAOP added that the privacy Instructions were not intended to change; any required changes would occur through Appendices. The SAOP further stated that the privacy office is in the process of reviewing the Guidance documentation to determine what they still need, or what they can streamline within the *NCUA Privacy Program Plan*; they would update any remaining Guidance or Instructions via Appendices as necessary.

NIST Special Publication 800-53, Revision 4, Privacy Control AR-1 - Governance and Privacy Program Control, requires organizations to update their privacy plan, policies and procedures on an organizationally defined frequency, but at least biennially.

Keeping privacy-related policies and procedures up-to-date will help the agency ensure it accurately reflects and disseminates current privacy control requirements. More importantly, up-to-date policies and procedures will provide greater assurance that employees and contractors are performing tasks with clear direction, potentially increasing the proper handling of PII, mitigating harm to individuals, loss of public trust in the NCUA or credit unions, and legal liability or increased costs of the NCUA or credit unions associated with a breach of PII.

To assist the NCUA in strengthening its privacy monitoring program, we recommend that NCUA management:

Recommendation 10: *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.*

Agency Response:
Management concurred with the recommendation. Management indicated that by September 30, 2020, the NCUA will implement a Privacy Continuous Monitoring Strategy based on NIST Special Publication 800-53, Rev 4.

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

Recommendation 11: *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.*

Agency Response:
Management concurred with the recommendation. Management indicated that by September 30, 2020, the NCUA will leverage automated tools to measure the effectiveness of privacy activities and compliance.

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

Recommendation 12: *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.*

Agency Response:
Management concurred with the recommendation. Management indicated that by June 30, 2020, the NCUA will issue a report documenting review of privacy policies and procedures.

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

Security Function: Detect

5. The NCUA Needs to Maintain its Security Authorization Process in Accordance with NIST Requirements

FY 2019 IG FISMA Metric Area: *Information Security Continuous Monitoring*

We noted the following issues regarding the security authorization process:

- The NCUA had a change in AOs and did not issue new authorization decision documents for the following systems since the previous AO left the agency in October 2018: 1) GSS, 2) AIRES, 3) CUOnline, 4) IIS, 5) CUSO Registry, and 6) ALMS.

  OCIO management informed us that when the incumbent CIO appointed the CISO as the new AO, the CISO had evaluated the status of the NCUA's system Authorization to Operate (ATO) and determined which systems had expiring ATOs. OCIO management informed us it had prioritized signing those system ATOs that were expiring and deferred the systems that did not have expiring ATOs, which are the systems we reviewed during the audit.

- The incumbent CIO designated the CISO as the new AO effective November 2018, contradictory to NIST requirements.

  The CIO informed us he made a decision to delegate the AO responsibilities to the CISO because he was familiar with other agency CIOs delegating this responsibility to the CISO. In addition, the CISO was acting as the Information Technology and Assurance Division (ITA) Director, who was designated as the AO, while the vacant position was filled. When we discussed this with the CIO during the audit, he indicated that the designation was due to resource constraints with the vacant ITA Director position and he did not realize this created a conflict of interest.

OMB Circular A-130, Appendix I, states: "In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the continuous monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system or the common controls and explicitly accepting the risk. If the new authorizing official is not willing to accept the previous authorization results (including the identified risk), a reauthorization action may need to be initiated or the new authorizing official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date."

Additionally, NIST SP 800-37 Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* Feb. 2010, describes a security authorization as the "official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls." Appendix F, Section 5 of NIST SP 800-37 addresses reauthorization decisions and states that they "can be either time driven or event driven. Event–driven triggers include a change in the authorizing official."

Furthermore, NIST SP 800-37 states:

"The senior information security officer is an organizational official responsible for: (i) carrying out the chief information officer security responsibilities under FISMA; and (ii) serving as the primary liaison for the chief information officer to the organization's authorizing officials, information system owners, common control providers, and information system security officers."

"The senior information security officer (or supporting staff members) may also serve as authorizing official designated representatives or security control assessors."

"The *authorizing official designated representative* is an organizational official that acts on behalf of an authorizing official to coordinate and conduct the required day-to-day activities associated with the security authorization process." "The only activity that cannot be delegated to the designated representative by the authorizing official is the authorization decision and signing of the associated authorization decision document (i.e., the acceptance of risk to organizational operations and assets, individuals, other organizations, and the Nation)."

By following OMB and NIST requirements when there is a change in the AO, the NCUA ensures that an appropriate senior official is accountable for ongoing acceptance of the identified risks and held responsible for the information systems. In addition, by separating duties between the CISO and the AO, the CISO will be able to more effectively carry out the primary responsibility of maintaining information security for the agency so the AO can focus on making ongoing credible, risk-based decisions for the NCUA's systems that support the business operations they are responsible for.

Furthermore, if the CISO is also the authorizing official, there is an increased risk that the NCUA will not have proper oversight of the security authorization process and the CISO would be making authorization decisions for information systems he is not operationally responsible for.

To assist the NCUA in strengthening the information system security authorization process we recommend that NCUA management:

> ***Recommendation 13****: Appoints an authorizing official that is in line with NIST 800-37, Risk Management Framework for Information Systems and Organizations, Revision 2.*
>
> ***Recommendation 14****: Ensures the new authorizing official completes the process of reauthorizing all of the NCUA's information systems by signing new authorization decision documents.*

Agency Response:
Management concurred with the recommendation. Management indicated that by March 31, 2020, the NCUA will appoint an Authorizing Official and reauthorize all information systems.

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

6. The NCUA Needs to Strengthen its Security Control Assessment Process

FY 2019 IG FISMA Metric Area: *Information Security Continuous Monitoring*

The NCUA did not conduct an annual SCA for IIS since it was removed from the three year security authorization cycle to an ongoing authorization. The NCUA conducted the last SCA in May 2018.

NCUA management stated that the IIS System Security Plan was reviewed and updated. However NCUA management informed us they were not aware of the need to assess controls for operating effectiveness on an ongoing basis for systems under ongoing authorization.

NIST SP 800-53, Revision 4, requires organizations to develop a continuous monitoring strategy and implement a continuous monitoring program that includes assessing and analyzing security controls and information security-related risks on an ongoing basis in accordance with the organization's continuous monitoring strategy.

The *NCUA Information Security Procedural Manual* requires an annual assessment of the information system security controls. The ISSO is responsible for ensuring the assessment is completed.

By conducting annual security control assessments of the agency's information systems, the system owner will have greater insight into which controls are not implemented correctly, operating as intended, and producing the desired outcome in meeting security requirements. This information will assist the system owner in focusing the proper resources on areas of greatest risk to ultimately strengthen the security posture of the information system.

To assist the NCUA in strengthening the security control assessment process we recommend that NCUA management:

Recommendation 15*: Ensures annual independent security control assessments are conducted for all agency information systems.*

Agency Response:
Management concurred with the recommendation. Management indicated that by June 30, 2020, the NCUA will update the NCUA information security policy and ensure independent security control assessments are conducted for all agency information systems.

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

Appendix I

BACKGROUND

National Credit Union Administration

The NCUA is the independent federal agency that charters, supervises, and insures the nation's federal credit unions. The NCUA also insures many state-chartered credit unions. The NCUA's operating fund contains the attributes of a revolving fund,[10] which is a permanent appropriation. The NCUA is authorized to collect annual operating fees from sources outside of congressional appropriations, define the purpose for which these collections may be used, and use the collections without fiscal year limitation. 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 October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*. This

[10] 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."

memorandum describes the processes for Federal agencies to report to OMB and, where applicable, DHS. Accordingly, the FY 2019 IG FISMA Reporting Metrics, provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[11]

The FY 2019 IG FISMA Reporting Metrics incorporate a maturity model that aligns with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework or CSF), version 1.1 Identify, Protect, Detect, Respond and Recover. The CSF provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise information technology and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 3**.

Table 3: Aligning the NIST Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

NIST Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metrics Domains
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 2019 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*.

Table4: 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.

[11] https://www.dhs.gov/publication/fy19-fisma-documents

Appendix I

Maturity Level	Maturity Level Description
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.

Appendix II

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

CLA conducted this audit in accordance with GAGAS. Those standards require that the auditor plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for their findings and conclusions based on the audit objective. CLA believes that the evidence obtained provides a reasonable basis for CLA's findings and conclusions based on the audit objective.

The scope of the audit included assessing select NIST 800-53, Revision 4 security and privacy controls mapped to the following FY 2019 IG FISMA Reporting Metrics domains for six 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 six NCUA information systems were selected for review from the 33 information system in the NCUA's system inventory:

- GSS
- AIRES
- CUOnline
- IIS
- ALMS
- 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.[12] Audit fieldwork was performed at the NCUA's headquarters in Alexandria, VA from June 12, 2019 to September 30, 2019. It covered the period from October 1, 2018, through September 30, 2019.

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) plan 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 2019 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 1, *Guide for Applying the Risk Management Framework to Federal Information Systems,* 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.

[12] *FY 2018 Independent Evaluation of the National Credit Union Administration's Compliance with the Federal Information Security Modernization Act of 2014* (Report #OIG-18-07, October 31, 2018).

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 2018 FISMA audit.[13] During FY 2019, the NCUA implemented corrective actions to close five prior year recommendations from the FY 2018 FISMA evaluation.

Finding #	Recommendation	Status
2017-4	The NCUA System Owners, in coordination with the Office of the Chief Information Officer, document and implement role-based account management procedures including but not limited to authorizing, creating, modifying, disabling, removing, logging and reviewing system accounts in accordance with the NCUA policy.	Closed
2018-1	The Office of the Chief Information Officer update the OCIO NCUA Information Systems Security Manual to establish a timeframe within which System Owners document the system risk assessments and Plan of Action and Milestones after completing security control assessments.	Closed
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.	Open See finding 1
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.	Open See finding 1
2018-4	The Office of the Chief Information Officer ensure the Office of the Chief Information Officer (OCIO) National Credit Union Administration (NCUA) Information Systems Security Manual addresses documenting security impact analysis results and the level of detail required.	Closed

[13] Ibid. footnote 11

Appendix III

Finding #	Recommendation	Status
2018-5	The Office of the Chief Information Officer ensure configuration management procedures address explicit review and discussion of the security impact analysis results prior to approving or denying system changes.	Closed
2018-6	The Office of Continuity and Security Management complete its employee background re-investigations.	Open Based on the corrective action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2022.
2018-7	The Office of Continuity and Security Management work with the Office of Human Resources to improve the notification process for when employees transfer to new positions.	Closed
2018-8	The Office of the Chief Information Officer enforce the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.	Open Based on the correct action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2019.
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 Based on the correct action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2019.
2018-10	The Office of the Chief Information Officer implement a process to identify authorized software in its environment and remove any	Open

Appendix III

Finding #	Recommendation	Status
	unauthorized software.	Based on the correct action plan provided by NCUA management, this issue was not scheduled for completion until December 31, 2019.

Appendix IV

MANAGEMENT COMMENTS

National Credit Union Administration
Office of the Executive Director

SENT BY E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel

SUBJ: Management Response – FY 2019 Federal Information Security Modernization Act (FISMA) of 2014 Audit

DATE: December 5, 2019

The following is the response to recommendations set forth in the Office of Inspector General's draft report titled *National Credit Union Administration Federal Information Security Modernization Act of 2014 Audit, Fiscal year 2019*. NCUA concurs with the report's recommendations.

OIG Report Recommendations #1, #2, and #3

1. Ensure the Agency addresses all control weaknesses documented in the system security plans and security assessment reports in their Plan of Action and Milestones.

2. Ensure the Agency timely and adequately manages and maintains the completion dates within the Plan of Action and Milestones.

3. Ensure the Agency performs likelihood analysis on all known vulnerabilities from all sources as part of its information system risk assessment.

Response: By December 31, 2020, NCUA will implement a quality assurance review to improve system security documentation, including identifying control weaknesses and establishing Plan of Action and Milestones resulting from security controls assessments. NCUA will manage Plan of Action and Milestone completion dates in accordance with NCUA policy, and will review and update the assessment and authorization procedures to ensure the likelihood analyses are consistently performed and documented in the information system risk assessment.

OIG Report Recommendations #4, #5, and #6

4. Ensure the Agency implements, tests, and monitors [redacted] in the NCUA information technology environment in compliance with established NCUA security standards. This includes documenting approved deviations from the [redacted] with business justifications.

5. Ensure the Agency maintains and reviews test results in ServiceNow for all system changes.

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

6. Ensure the Agency completes and documents a security impact analysis for emergency changes in accordance with the OCIO Operational Change Control Board Charter.

Response: By December 31, 2024, NCUA will implement, test, and monitor [redacted] in the NCUA information technology environment in compliance with established NCUA security standards.

By December 31, 2020, NCUA will implement a quality review process to ensure test results are maintained and reviewed in ServiceNow for all system changes and will update policies and procedures to ensure security impact analysis results are captured and incorporated into its change process for emergency changes.

OIG Report Recommendations #7, #8, and #9

7. Ensure the CUSO Registry system owner obtains a risk acceptance from the Authorizing Official for the deviation from NCUA policy for inactive accounts.

8. Ensure the CU Online and CUSO Registry system owner restricts access to non-public data to only those users who require it, in accordance with the concept of least privilege.

9. Ensure 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.

Response: Operations of CUOnline and the CUSO Registry currently require different account management processes. Both of these systems are included in the agency's roadmap for business system modernization.

By June 30, 2020, NCUA will ensure the CUSO Registry system owner obtains a risk acceptance from the Authorizing Official for the deviation from NCUA policy for inactive accounts and the CU Online and CUSO Registry system owners obtain a risk acceptance from the Authorizing Official for the deviation from NCUA policy for least privilege.

By June 30, 2020, the NCUA will review and update the information security policy and procedures, as required, to ensure that signed information system access agreements are documented and maintained.

OIG Report Recommendations #10, #11, and #12

10. Ensure 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.

11. Ensure 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.

12. Ensure 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.

Response: NCUA's Privacy Continuous Monitoring Strategy (PCMS) will include a formal process for assessing agency privacy controls on at least an annual basis and will leverage automated tools to measure the effectiveness of privacy activities and compliance. NCUA will implement PCMS by September 30, 2020 based on NIST Special Publication 800-53, Rev 4.

By June 30, 2020, the agency will issue a report documenting the enterprise and office level review of privacy policies and procedures. The report will identify a streamlined approach for implementing a consistent, comprehensive privacy framework.

OIG Report Recommendations #13 and #14

13. Appoint an authorizing official that is in line with NIST 800-37, Risk Management Framework for Information Systems and Organizations, Revision 2.

14. Ensure the new authorizing official completes the process of reauthorizing all of the NCUA's information systems by signing new authorization decision documents.

Response: The NCUA will appoint an Authorizing Official and will reauthorize all information systems by March 31, 2020.

OIG Report Recommendation #15

15. Ensure that annual independent security control assessments are conducted for all agency information systems.

Response: NCUA will review and update the NCUA information security policy and ensure independent security control assessments are conducted for all agency information systems in accordance with the NCUA information security policy by June 30, 2020.

Thank you for the opportunity to review and comment. If you have any questions, please contact my office.