



NCUA
National Credit Union Administration

**OFFICE OF INSPECTOR
GENERAL**

**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**



TABLE OF CONTENTS

Section	Page
EXECUTIVE SUMMARY	1
BACKGROUND	2
RESULTS IN DETAIL.....	4
Continuous Monitoring Program Needs Strengthening.....	4
Recommendations 1, 2, & 3.....	8
Security Impact Analysis for System Changes Not Documented	9
Recommendations 4 & 5.....	11
Personnel Background Investigations Not Completed	11
Recommendations 6 & 7.....	13
Network Vulnerabilities Not Remediated.....	14
Recommendations 8, 9 & 10.....	17
Unresolved FY 2017 Recommendation.....	18
APPENDICES:	
A. Objective, Scope, and Methodology	19
B. Acronyms and Abbreviations	21
C. NCUA Management Response	23



EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged CliftonLarsonAllen LLP (CLA) to independently evaluate the NCUA's information security and privacy management programs and controls for compliance with the Federal Information Security Modernization Act of 2014 (FISMA 2014) and federal regulations and standards.

CLA evaluated the NCUA's information security and privacy management programs through interviews, documentation reviews, technical configuration reviews, and sample testing. This year, CLA also conducted a vulnerability assessment of NCUA's network. CLA evaluated the NCUA against such laws, standards, and requirements as those provided through FISMA 2014, the E-Government Act, National Institute of Standards and Technology (NIST) standards and guidelines, the Privacy Act, and Office of Management and Budget (OMB) memoranda and privacy and information security policies.

In addressing and resolving prior year issues and recommendations, the NCUA has continued to strengthen its information security program during Fiscal Year (FY) 2018. Specifically, the NCUA:

- Has addressed and closed its six remaining recommendations from the FY 2016 FISMA report.
- Has addressed and closed seven of its eight recommendations from the FY 2017 FISMA report. OCIO provided documentation that it indicates supports closure of the remaining recommendation. However, the OIG received this documentation too late for CLA to adequately and fully assess it for this FISMA reporting year. The OIG will assess the documentation during FISMA 2019 to determine the status of this recommendation.

In this year's FISMA review, we identified areas for improvement in information security continuous monitoring, configuration management, personnel security, and risk management. We made 10 recommendations, which should help the NCUA continue to improve the effectiveness of its information security program. We have included the NCUA's comments in their entirety at Appendix B.

We appreciate the courtesies and cooperation provided to our staff and CLA staff during this review.



BACKGROUND

This section provides background information on FISMA 2014 and the NCUA.

Federal Information Security Modernization Act of 2014

The President signed into law the E-Government Act of 2002 (Public Law 107-347) on December 17, 2002, which includes Title III, Information Security (the Federal Information Security Management Act). The Federal Information Security Management Act (FISMA) permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000, which expired in November 2002. FISMA charged the Office of Management and Budget (OMB) with oversight of information security policies and practices.

On December 18, 2014, the President signed FISMA 2014 into law (Public Law 113-283), which reformed FISMA. FISMA 2014 authorizes the Secretary of the Department of Homeland Security (DHS) to assist the OMB Director in administering the implementation of agency information and security practices for federal information systems. Among other changes, FISMA 2014 also:

- Changes agency reporting requirements, modifying the scope of reportable information from primarily policies and financial information to specific information about threats, security incidents, and compliance with security requirements.
- Updates FISMA to address cyber breach notification requirements.
- Required the OMB Director to – within one year of the enactment of FISMA 2014 – revise Office of Management and Budget Circular A-130 to eliminate inefficient or wasteful reporting.¹

On October 16, 2017, OMB issued Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirement (M-18-02). This memorandum provides agencies with FY 2018 Federal Information Security Modernization Act and Privacy Management reporting guidance and deadlines as required by FISMA 2014. In addition, the memorandum consolidates requirements from prior OMB annual FISMA guidance to ensure consistent, government-wide performance and agency adoption of best practices; and rescinds the following prior year annual FISMA memoranda: OMB M-15-01, OMB M-16-03, and OMB M-17-05. On May 24, 2018, DHS issued the FY 2018 reporting metrics, which provide the

¹ OMB published the revised Circular A-130, Managing Information as a Strategic Resource, on July 28, 2016.



reporting requirements across key areas. Inspectors General are to address in independently evaluating agencies' information security programs.²

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,³ 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."

The NCUA's primary function is to identify credit union system risks, determine the magnitude, and mitigate unacceptable levels through the examination and supervision program. The NCUA strives to effectively manage the balance between regulatory flexibility and responsible oversight.

The NCUA has a full-time three-member Board (NCUA Board) consisting of a chairman and two members. The President of the United States appoints the members of the board and the Senate confirms the board members. No more than two board members can be from the same political party, and each member serves a staggered six-year term. The NCUA Board meets regularly each month in Alexandria, Virginia in open session, with the exception of August.

² FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1 (May 24, 2018)

³ 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."



RESULTS IN DETAIL

Information security and privacy program planning and management controls are designed to provide the framework and continuing cycle of activity for managing risk, developing security and privacy policies, assigning responsibilities, and monitoring the adequacy of information security-related and privacy-related controls. The NCUA has addressed all six recommendations remaining from the 2016 FISMA report and has addressed seven of the eight recommendations from the FY 2017 FISMA report. OCIO management informed us that it has addressed that remaining recommendation and provided the documentation for CliftonLarsonAllen, LLP (CLA) to assess. Because CLA received the documentation after the end of field work, the contractor was unable to assess it for the 2018 FISMA reporting year. We will assess the documentation during the 2019 FISMA reporting year to determine whether NCUA actions have resolved the recommendation.

This year we identified four findings and 10 recommendations within the following areas: information security continuous monitoring, configuration management, personnel security, and risk management. We discuss the new issues and the unresolved recommendation from 2017 below.

Continuous Monitoring Program Needs Strengthening

We determined the NCUA did not effectively manage some elements of its continuous monitoring process. Specifically, NCUA did not timely complete or adequately manage its system risk assessments and Plan of Action and Milestones (POA&Ms) to successfully mitigate and manage risk as indicated below:

- The NCUA has not fully documented its General Support System (GSS) and Insurance Information System (IIS) system risk assessments and POA&Ms after completing the Security Control Assessments (SCA) in November 2017 and May 2018, respectively. Specifically, we noted the following:
 - GSS:
 - The system risk assessment did not address [REDACTED] security controls that the NCUA listed in the System Security Plan (SSP) as not implemented; in the Security Assessment Report (SAR) as not fully satisfied; or as open POA&Ms.
 - The POA&Ms did not include [REDACTED] security controls that the NCUA listed in the SSP as not implemented and did not include [REDACTED] security controls the NCUA listed in the SAR as not fully satisfied.



- IIS:
 - The system risk assessment did not address [REDACTED] security controls the NCUA listed in the SSP as not implemented; in the SAR as not fully satisfied; or as open POA&Ms.
 - The POA&Ms did not include [REDACTED] security control that the NCUA listed in the SSP as not implemented and did not include [REDACTED] security controls the NCUA listed in the SAR as not fully satisfied.
- The NCUA did not adequately manage its POA&M completion dates. Specifically, the NCUA did not meet a number of scheduled dates for completing POA&Ms, and did not document new completion dates for the following systems:
 - GSS - [REDACTED]
 - Automated Integrated Regulatory Examination System (AIRES) - [REDACTED]
 - Credit Union Online (CU Online) - [REDACTED]
 - CUSO Registry (CUSO) - [REDACTED]
 - Asset Liability Management System (ALMS) - [REDACTED]

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to develop a continuous monitoring strategy and implement a continuous monitoring program that includes: 1) assessing and analyzing security controls and information security-related risks on an ongoing basis in accordance with the organization's continuous monitoring strategy; 2) generating response actions to address results of the risk-based analysis of security-related information; and (3) reporting the security status of the organization and the information system.

NIST 800-53, Revision 4 also:

- Requires organizations to define the frequency to update its risk assessments whenever there are significant changes to the information system or environment of operation (including the identification of new threats and vulnerabilities); and whenever there are other conditions that may impact the security state of the system.
- Requires organizations to define the frequency to update its plan of action and milestones based on findings from security control assessments, security impact assessments, and continuous monitoring activities.
- Indicates that as an organization's assessment and authorization process relies to a greater degree on continuous monitoring, the ability to update the security and privacy



assessment reports frequently becomes a critical aspect of information security and privacy programs.

NIST SP 800-30, Revision 1, *Guide for Conducting Risk Assessments*, indicates risk assessments address the potential adverse impacts to organizational operations and assets, individuals, other organizations, and the economic and national security interests of the United States, arising from the operation and use of information systems and the information processed, stored, and transmitted by those systems. Organizations conduct risk assessments to determine risks that are common to the organization's core missions/business functions, mission/business processes, mission/business segments, common infrastructure/support services, or information systems.

NIST SP-800-30, Revision 1 also indicates "[t]o maximize the benefit of risk assessments, organizations should establish policies, procedures, and implementing mechanisms to ensure that the information produced during such assessments is effectively communicated and shared...to ensure that decision makers across the organization have the appropriate risk-related information needed to inform and guide risk decisions."

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations*, states: "Response strategies may be implemented over a period of time, documenting implementation plans in the system's Plan of Action and Milestones. As weaknesses are found, response actions are evaluated and any mitigation actions are conducted immediately or are added to the POA&M." NIST defines a POA&M as: "A document that identifies tasks needing to be accomplished. It details resources required to accomplish the elements of the plan, any milestones in meeting the tasks, and scheduled completion dates for the milestones."

NIST SP 800-137 also indicates organizations report security-related information generated from security control assessments in accordance with organizational policies and procedures to help ensure that risk-based decisions are informed by accurate, current security-related information.

In addition, the *Office of the Chief Information Officer (OCIO) National Credit Union Administration (NCUA) Information Systems Security Manual (Manual)*, states "The implementation of a continuous monitoring program must result in ongoing updates to the SSP, SAR, and POA&M."

The Manual also requires risk assessments to list each control required by NIST SP 800-53 including the implementation status (i.e., not in place, planned, implemented) of the control.

Finally, the Manual requires the development of POA&Ms to document the planned, remedial actions to correct weaknesses or deficiencies in security controls. POA&Ms are the responsibility of the System Owner.

OCIO management told us the delay in completing the risk assessments and POA&Ms associated with the fiscal year 2018 SCAs for the GSS and ISS was to provide enough time for a



quality review process to ensure the security documentation was compliant with NIST standards. OCIO management also indicated that although they had not documented the control weaknesses in the risk assessment and POA&Ms, corrective action was ongoing. We noted however, that the Information System Security Officers (ISSO) for each of the systems had not documented plans to support any ongoing corrective actions.

In addition, OCIO management informed us:

- ISSOs are responsible for briefing the Chief Information Security Officer (CISO) on the status of POA&Ms and for updating the POA&Ms once the CISO approves new dates.
- At the time, the individuals listed as ISSOs in the system security plans had other responsibilities, which limited the time and attention they were able to dedicate to accomplish their ISSO duties related to managing the POA&Ms. As a result, the ISSOs had not worked with the CISO to establish updated completion dates.
- The NCUA had been in the process of addressing the lack of dedicated ISSOs since last year. Specifically:
 - NCUA was hiring ISSOs who would be solely dedicated to supporting the agency's information system's assessment and monitoring process.
 - The hiring process was delayed, but NCUA onboarded the ISSOs at the end of September 2018.
- They expect that having dedicated ISSOs will improve the agency's ability to adhere to its continuous monitoring processes.

Finally, the *Office of the Chief Information Officer (OCIO) National Credit Union Administration (NCUA) Information Systems Security Manual* does not address a timeline for addressing control weaknesses in documented risk assessments and POA&Ms after completing the SCAs.

By adequately and timely 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, 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 NCUA's information and information systems.



We recommend that:

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.

Agency Response:

Management concurred with the recommendation. Management indicated that by June 30, 2019, the Office of the Chief Information Officer will review and update its policies and procedures in accordance with applicable standards.

OIG Response:

We concur with management's planned action.

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

Agency Response:

Management concurred with the recommendation. Management indicated that by June 30, 2019, the Office of the Chief Information Officer will ensure system owners for the GSS and the IIS address all control weaknesses in the system security plans and security assessment reports. Management indicated that in addressing the control weaknesses, the Office of the Chief Information Officer will document its actions, including mitigation, acceptance of risk, etc., as applicable.

OIG Response:

We concur with management's planned action.

3. The NCUA management ensure the system owners timely and adequately manage and maintain the completion dates within the Plan of Action and Milestones.

Agency Response:

Management concurred with the recommendation. Management indicated that by June 30, 2019, the Office of the Chief Information Officer will ensure system owners manage completion dates within the Plan of Action and Milestones.

OIG Response:

We concur with management's planned action.



Security Impact Analysis for System Changes Not Documented

We determined the NCUA did not have documentation detailing a security impact analysis (SIA) the Director of Information Technology Assurance would have considered when the Operational Change Control Board (CCB) voted to approve or deny system change requests. Specifically, NCUA did not have documentation to validate that it performed an SIA on any of the sample of 48 [of the total population of 212] system change requests we tested. The following summarizes the sample of 48 change request packages we reviewed:

- General Support System (GSS) – 13
- Automated Integrated Regulatory Examination System (AIRES) - 10
- Insurance Information System (ISS) - 5
- Credit Union Service Organization (CUSO) Registry System - 10
- Credit Union (CU) Online - 10

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires organizations to: (1) review proposed configuration-controlled changes to the information system and approve or disapprove such changes with *explicit* [emphasis added] consideration for security impact analyses; and (2) analyze changes to its information systems to determine potential security impacts due to flaws, weaknesses, incompatibility, and intentional malice prior to implementing the changes.

NIST SP 800-128, *Guide for Security-Focused Configuration Management of Information Systems*, states:

- “Security impact analysis is the analysis conducted by qualified staff within an organization to determine the extent to which changes to the information system affect the security posture of the system. Because information systems are typically in a constant state of change, it is important to understand the impact of changes on the functionality of existing security controls and in the context of organizational risk tolerance. Security impact analysis is incorporated into the *documented* [emphasis added] configuration change control process.”
- “The analysis of the security impact of a change occurs when 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. Once the changes are implemented and tested, a security impact analysis (and/or assessment) is performed



to ensure that the changes have been implemented as approved, and to determine if there are any unanticipated effects of the change on existing security controls.”

- “Configuration Change Control...procedure includes, but is not limited to...[s]ecurity impact analysis procedures including how and with what level of rigor analysis results are to be documented and requirements for post-implementation review to confirm that the change was implemented as approved and that no additional security impact has resulted....”
- Conducting the security impact analysis is one of the most critical steps in the configuration change control process with respect to security focused configuration management.

The *Office of the Chief Information Officer (OCIO) National Credit Union Administration (NCUA) Information Systems Security Manual*, Control CM-4a– Security Impact Analysis, requires: (a) personnel with information security responsibilities (e.g., Network/System Administrators, Information System Security Officers, and Information System Security Engineers) analyzed system changes to determine potential security impacts; and (b) the SIA be provided to the Information System Security Officer (ISSO) to ensure that the ISSO is aware of any changes to the security controls which may impact the security posture of the information system.

Although OCIO management indicated that as a member of the OCIO CCB, the Director of Information Technology Assurance takes into account impact to security controls when voting to approve or deny system changes, OCIO management was unable to provide documentation to show what security impacts the CCB considered.

NCUA’s *OCIO Information Systems Security Manual* does not address: a) documenting SIA results and the level of detail required; or b) presentation and discussion of documented SIAs during CCB meetings before the change is deployed.

In addition, key change management documentation either does not address SIAs, or does not address SIAs in sufficient detail. For example:

- The *Office of Chief Information Officer (OCIO) Operational Change Control Board (CCB) Charter* does not address review and discussion of security impact analysis results prior to approving or denying system changes.
- The *General Support System Configuration Management Plan* requires the ISSO to conduct an SIA; however, it does not address the level of rigor of the SIA and how the ISSO is to document the results of the SIA.



By enhancing its security-focused configuration management procedures to include documenting the detailed analysis of the security impact of changes on NCUA systems, 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.

We recommend that:

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.

Agency Response:

Management concurred with the recommendation. Management indicated that by June 30, 2019, the Office of the Chief Information Officer will review and update the policies and procedures to ensure security impact analysis results are captured and incorporated into its change management process in accordance with applicable federal standards.

OIG Response:

We concur with management's planned action.

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.

Agency Response:

Management concurred with the recommendation. Management indicated that by June 30, 2019, the Office of the Chief Information Officer will review and update the policies and procedures to ensure security impact analysis results are captured and incorporated into its change management process in accordance with applicable federal standards.

OIG Response:

We concur with management's planned action.

**Personnel Background
Investigations Not
Completed**

We determined NCUA did not always ensure employees had the proper background investigations. Specifically, three employees from a sample of 25 employees with access to the NCUA network had background investigations at a lower level than the risk associated with their assigned positions as noted

in their Position Designation Automated Tool (PDAT). One individual had a Tier 1 investigation, while the investigation level required on the PDAT was Tier 2, and the other two individuals had a Tier 2 investigation, while the investigation required on the PDAT was Tier 4.



National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, requires the organization: a. Screens individuals prior to authorizing access to the information system; and b. Rescreens individuals according to [Assignment: organization-defined conditions requiring rescreening and, where rescreening is so indicated, the frequency of such rescreening].

The Office of the Chief Information Office (OCIO) National Credit Union (NCUA) Information Systems Security Manual, provides the control requirements for Personnel Screening which include:

“The organization:

- a. Screens individuals prior to authorizing access to the information system;
- b. Rescreens individuals anytime they move to a new position with a higher risk designation;
- c. Conducts background investigations in a manner commensurate with OPM and NCUA Human Resources policy and guidance;
- d. Performs reinvestigations in accordance with guidance provided by current personnel security policy; and
- e. Refuses employees and contractors access to information systems until they have:
 1. Been granted an interim clearance, and
 2. Signed the appropriate access agreements.”

In December 2011, OPM released a new regulation that required background re-investigations (investigations) on agencies' Public Trust positions every five years. This regulation required the Office of Continuity and Security Management (OCSM) to begin re-investigations on a large population of its employees.

During FY 2016, OPM released guidance requiring agencies to review *all* positions utilizing the OPM Position Designation Automated Tool (PDAT). The Office of Human Resources (OHR) began reviewing all positions. OCSM decided to pause its backlog of investigations of employees in Public Trust positions until OHR could complete its review of the positions. OCSM management stated the review had a very low impact on the risk designations and did not have a significant impact on the existing backlog of employees requiring investigations.



During 2017, OHR completed its review of all positions, at which time OCSM resumed investigating the residual backlog of approximately 400 employees. OCSM staff is completing this large volume of required investigations with existing resources.

In addition, one of the three individuals we sampled changed to a position requiring a higher (Tier 2) investigation than the employee's original Tier 1 position. OCSM management indicated they may not have received notification of this position change from OHR. OHR's manual process to inform OCSM when employees transfer to new positions may have contributed to this oversight.

By screening its employees, NCUA can validate that individuals are suitable for the level of system access or job responsibilities assigned to them. Ultimately, this helps protect the confidentiality, integrity and availability of NCUA's data and systems.

We recommend that:

6. The Office of Continuity and Security Management complete its employee background re-investigations.

Agency Response:

The OCSM will complete employee background re-investigations by December 31, 2022.

OIG Response:

We concur with Management's planned actions.

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.

Agency Response:

Management indicated it believes that process improvements the NCUA has made to automate HR Links reports that list employees transferring to new positions has resolved this recommendation.

OIG Response:

Since this action was taken subsequent to completing fieldwork for this year's FISMA review, we will review this response during FISMA 2019.



Network Vulnerabilities Not Remediated

We determined the NCUA had unpatched software, unsupported software, and improper configuration settings that exposed its Headquarters network to [REDACTED]

[REDACTED] Specifically, our scan of [REDACTED] computing devices identified [REDACTED]

[REDACTED] related to patch management, configuration management, and unsupported software. We identified [REDACTED] instances of these [REDACTED] unique vulnerabilities. Some of these unique vulnerabilities included:

- **Patch Management:** [REDACTED] which comprise half of the patch management vulnerabilities.

- **Configuration Weaknesses:** The majority of the configuration weaknesses [REDACTED]. There were also configuration weaknesses related to S [REDACTED]

Two high risk configuration vulnerabilities - [REDACTED]

A third high risk configuration vulnerability - [REDACTED]

- **Unsupported Software:** The unsupported software on NCUA's network included:

[REDACTED]

[REDACTED]

[REDACTED]

[REDACTED]

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, security control security control SI-2 states the following regarding patch management:

[REDACTED]



“The organization:

- c. Installs security-relevant software and firmware updates within [Assignment: organization defined time period] of the release of the updates.”

Office of Management and Budget, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, states:

- i. “Specific Safeguarding Measures to Reinforce the Protection of Federal Information and Information Systems

Agencies shall:

- 8. 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;
- 9. Implement and maintain current updates and patches for all software and firmware components of information systems.”

The Office of the Chief Information Officer (OCIO) National Credit Union Administration (NCUA) *Information Systems Security Manual*, Control RA-5 – Vulnerability Scanning states:

“Legitimate vulnerabilities must be added to the system POA&M for correction or mitigation as follows:

- i. Critical or High Vulnerabilities – These must be reported immediately when verified. S[ystem] O[w]ners have 30 days to correct these, after which a POA&M must be established.
- ii. Moderate Vulnerabilities – These must be corrected within 60 days after which a POA&M must be established.
- iii. Low Vulnerabilities – These must be corrected after high and moderate vulnerabilities are corrected as time permits. POA&Ms do not need to be established unless an aggregation of these vulnerabilities raises the risk to moderate or high.

The following corrective actions must be used when necessary as a result of vulnerability scanning results:

- i. Upgrade or patch vulnerable systems to mitigate identified vulnerabilities as appropriate.
- ii. Deploy mitigating measures (e.g., management, technical, procedural) if the system cannot be immediately patched (e.g., operating system upgrade will make the



application running on the operating system inoperable) in order to minimize the probability of this system being compromised. Mitigating controls satisfy “correction” of a vulnerability only if no control described in SP 800-53 applies or is available. For example, some vulnerabilities have published “workarounds” that may suffice until a technical solution is found. These may require an item in the POA&M.

- iii. Improve the change management and configuration management program and procedures and standards to ensure that systems are upgraded routinely with the latest solutions.
- iv. Assign a specified team or person(s) responsible for monitoring vulnerability alerts and mailing lists, examine applicability to the OCIO environment, and initiate appropriate system changes.
- v. Modify or recommend modifications to OCIO security policies, architecture, or other documentation, processes or procedures to ensure that security practices include timely system updates and upgrades.”

Although OCIO management indicated NCUA has compensating controls in place, including firewalls, intrusion detection systems (IDS), endpoint protection and vulnerability surveillance to provide enhanced monitoring and detection of suspected malicious activity, OCIO management indicated:

- Software vulnerabilities were present on the network because OCIO did not properly monitor and track approved and installed software, which allowed the installed software to deviate over time from the originally installed base image. This made it more difficult for OCIO to apply patches since there were several versions of the same software present on the network, as well as, some unauthorized software. OCIO management indicated it was only deploying patches for authorized software versions they tracked. Consequently, OCIO was not updating software that it was not tracking or unauthorized software.
- NCUA has been in the process of migrating Windows 7 workstations to Windows 10 since it began pilot deployment in November 2017, followed by full deployment starting in July 2018. The deployment was on-going during the time independent third parties performed their scans. To allow a more streamlined schedule, OCIO management stated it made the decision to [REDACTED]

By timely installing required patches, implementing secure configuration settings, and migrating to supported software, NCUA can mitigate 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.



We recommend that:

8. The Office of the Chief Information Officer enforce the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.

Agency Response:

Management concurred with the recommendation. Management indicated that by December 31, 2019, the Office of the Chief Information Officer will enforce its policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.

OIG Response:

We concur with management's planned action.

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.

Agency Response:

Management concurred with the recommendation. Management indicated that by December 31, 2019, the Office of the Chief Information Officer will develop and implement a process to manage unsupported software.

OIG Response:

We concur with management's planned action.

10. The Office of the Chief Information Officer implement a process to identify authorized software in its environment and remove any unauthorized software.

Agency Response:

Management concurred with the recommendation. Management indicated that by December 31, 2019, the Office of the Chief Information Officer will develop and implement a process to manage unauthorized software.

OIG Response:

We concur with management's planned action.



Unresolved FY 2017 Recommendation

Following is the one remaining open issue and recommendation from the FY 2017 FISMA report, NCUA's response and the current status of that recommendation:

Regarding the NCUA's account management issues, we recommended: 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.

In response, NCUA management concurred with the recommendation, indicating that by June 30, 2018, NCUA would: (1) conduct a feasibility analysis for each legacy system's role-based access controls; (2) document the specific role-based access process and technical approach for each system to include acceptance of risk; and (3) implement the documented processes and controls.

During this FISMA reporting year, management and staff from the Office of Examination and Insurance (E&I) informed us they have been working closely with OCIO management and staff to resolve this recommendation. Specifically, E&I management and staff indicated actions they took included:

- Creating a roles based account management process.
- Implementing an automated [REDACTED].
- Improving System Security Plan (SSP) documentation for account management access controls.
- Developing account management reports to conduct user account reviews.

CLA (the OIG's contractor) reviewed the SSPs for AIREs, CU Online and the CUSO Registry System and determined that while improved, the SSPs would need to include additional detail to resolve the recommendation. OCIO management informed us that OCIO and E&I staff updated the SSPs as of October 4, 2018, . OCIO provided the updated SSPs to CLA for review. CLA received the SSPs after the end of field work, which did not allow sufficient time for CLA to adequately and fully assess them for the 2018 FISMA reporting year. The contractor will assess OCIO's and E&I's continuing efforts and the SSPs during FISMA 2019 to determine whether NCUA actions will have resolved the recommendation.



Appendix A: Objective, Scope, and Methodology

The objective of this review was to perform an independent evaluation of the NCUA information security and privacy management programs and controls for compliance with FISMA 2014 and federal regulations and standards. We evaluated the NCUA's efforts related to:

- Efficiently and effectively managing its information security and privacy management programs;
- Meeting responsibilities under FISMA 2014; and
- Remediating prior weaknesses pertaining to FISMA 2014 and other information security and privacy weaknesses identified.

In addition, the review was required to provide sufficient supporting evidence of the status and effectiveness of the NCUA's information security and privacy management programs to enable reporting by the OIG.

We evaluated the NCUA's information security and privacy management programs and practices against such laws, standards, and requirements as those provided through FISMA 2014, the E-Government Act, National Institute of Standards and Technology's (NIST) standards and guidelines, the Privacy Act, and OMB memoranda and information security and privacy policies. This year we also conducted a vulnerability assessment of the NCUA's network.

During this review, we assessed the NCUA's information security program domains as identified in The Department of Homeland Security's FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (V1.0.1). The FISMA reporting metrics are organized around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity. These functions and corresponding metric domains include:

- Identify:
 - Risk Management and
 - Contractor Systems
- Protect:
 - Configuration Management,
 - Identify and Access Management, and
 - Security Training
- Detect:
 - Information Security Continuous Monitoring



- Respond:
 - Incident Response
- Recover:
 - Contingency Planning

We conducted our fieldwork from June 2018 through September 2018. In connection with the contract, we prepared this report in reliance upon the documentation and associated work of the Independent Public Account (IPA). We reviewed the IPA's related documentation and inquired of its representatives. Our review, as differentiated from an audit in accordance with generally accepted government auditing standards, was not intended to enable us to express, and we do not express, an opinion on the matters contained in the report. The IPA is responsible for the findings, recommendations, and conclusions contained in this report. However, our review disclosed no instances where the IPA did not comply, in all material respects, with generally accepted government auditing standards.



Appendix B: Acronyms and Abbreviations

Acronym	Term
AIRES	Automated Integrated Regulatory Examination System
ALMS	Automated Liquidation Management Services
CCB	Operational Change Control Board
CISO	Chief Information Security Officer
CLA	CliftonLarsenAllen, LLP
CU	Credit Union
CUSO	Credit Union Service Organization
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
E&I	Office of Examination and Insurance
FISMA	Federal Information Security Management Act
FISMA2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GSS	General Support System
IDS	Intrusion Detection System
IIS	Insurance Information System
Investigations	Background Investigations
ISSO	Information Systems Security Officer
Manual	Office of the Chief Information Officer National Credit Union Administration Information Systems Security Manual
MOU	Memorandum of Understanding
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology



Acronym	Term
OCIO	Office of the Chief Information Officer
OCSM	Office of Continuity and Security Management
OHR	Office of Human Resources
OIG	Office of Inspector General
OMB	Office of Management and Budget
PDAT	Position Designation Automated Tool
POA&M	Plan Of Action and Milestones
SAR	Security Assessment Report
SCA	Security Control Assessment
SIA	Security Impact Analysis
SP	Special Publication
SSA	State Supervisory Authority
SSP	System Security Plan

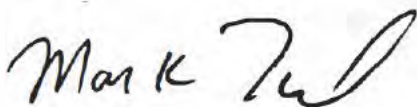
Appendix C: NCUA Management Response



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 2018 Federal Information Security Modernization Act (FISMA) of 2014 Compliance

DATE: October 29, 2018

The following is the response to recommendations set forth in the Office of Inspector General's draft report titled *FY 2018 Independent Evaluation of the NCUA's Compliance with FISMA*. NCUA concurs with the report's recommendations.

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

1. Update the Office of Chief Information Officer 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.
2. Ensure system owners for the GSS (OCIO) 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.
3. Ensure the system owners timely and adequately manage and maintain the completion dates within the Plan of Action and Milestones.

Response: By June 30, 2019, the OCIO will (1) review and update its policies and procedures in accordance with applicable federal standards, (2) ensure system owners for the GSS and the IIS address all control weaknesses in the system security plans and security assessment reports, and (3) ensure system owners manage completion dates within the Plan of Action and Milestones. In regards to recommendation 2, addressing these controls include a range of outcomes from full mitigating action to acceptance of the risk in the current state. We will document those decisions.

OIG Report Recommendation #4 and #5:

4. Ensure the OCIO NCUA Information Systems Security Manual addresses documenting security impact analysis results and the level of detail required.
5. Ensure configuration management procedures address explicit review and discussion of the security impact analysis results prior to approving or denying system changes.

Response: By June 30, 2019, the OCIO will review and update the policies and procedures to ensure security impact analysis results are captured and incorporated into its change management process in accordance with applicable federal standards.

OIG Report Recommendations #6 and #7:

6. Complete employee background re-investigations.
7. Improve the notification process between the Office of Continuity and Security Management (OCSM) and the Office of Human Resources when employees transfer to new positions.

Response: The OCSM will complete employee background re-investigations by December 31, 2022. Process improvements have been made to automate HR Links reports listing employees transferring to new positions, so we believe recommendation 7 has already been resolved.

OIG Report Recommendations #8, #9, and #10:

8. Enforce the policy to remediate patch and configuration related vulnerabilities within agency defined timeframes.
9. Implement a process to detect and migrate unsupported software to supported platforms before support for the software ends.
10. Implement a process to identify authorized software in its environment and remove any unauthorized software.

Response: By December 31, 2019, the OCIO will (1) enforce its policy to remediate patch and configuration related vulnerabilities within agency defined timeframes, (2) develop and implement a process to manage unsupported software, and (3) develop and implement a process to manage unauthorized software.

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