FY 2017
INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

REPORT #OIG-17-10
NOVEMBER 8, 2017

James W. Hagen
Inspector General

TABLE OF CONTENTS

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. 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) 2017. Specifically, the NCUA:

- Has addressed and closed the two remaining recommendations from the FY 2015 FISMA report.
- Has addressed and closed 17 of the 23 recommendations from the FY 2016 FISMA report, on or ahead of its planned timelines.
- Is in the process of addressing the six remaining recommendations from the FY 2016 FISMA report that the NCUA planned for completion after October 2017 (See Appendix A).

In this year's FISMA review, we identified areas for improvement in risk management, identify and access management, information security continuous monitoring, and security training. We made eight 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 C.

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

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]

DHS issued the FY 2017 reporting metrics, which provide measures against which agency Chief Information Officers, Inspectors General, and Senior Agency Officials for Privacy assess the status and compliance of agencies' information security and privacy management programs. 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 2017-2018 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

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

the following prior year annual FISMA memoranda: OMB M-15-01, OMB M-16-03, and OMB M-17-05.

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,[2] 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 foster the safety and soundness of federally insured credit unions and to better enable the credit union community to extend credit for productive and provident purposes to all Americans, particularly those of modest means.

The NCUA strives to ensure that credit unions are empowered to make necessary business decisions to serve the diverse needs of its members and potential members. It does this by establishing a regulatory environment that encourages innovation, flexibility, and a continued focus on attracting new members and improving service to existing members.

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] 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 the two recommendations remaining from the 2015 FISMA report and has addressed 17 of the 23 recommendations from the FY 2016 FISMA report, ahead of or on schedule. The NCUA is in the process of addressing the six remaining recommendations from the FY 2016 FISMA report as planned. This year we identified five findings and eight recommendations within the following FISMA domains: risk management, identify and access management, information security continuous monitoring, and security training. We discuss the new issues below and include the six unresolved prior year recommendations in Appendix A.

NIST Security Authorization Process Not Always Enforced

We determined the NCUA did not maintain current system authorizations to operate (ATO) for [redacted] information systems. In addition, the authorizing official signed ATOs for [redacted] systems without completed key security documents. Specifically:

Regarding [redacted] systems operating without a current ATO:

- The NCUA operated [redacted] for a period of six to seven months without an ATO. The ATOs for the following systems expired on December 15, 2016:
  - [redacted] The authorizing official signed a new ATO on July 31, 2017.
  - [redacted] The authorizing official signed a new ATO on June 19, 2017.
- The ATOs for the following [redacted] also expired on December 15, 2016. The NCUA has not issued current ATOs:
  - [redacted]
  - [redacted]
  - [redacted]

Regarding [redacted] ATOs the authorizing official signed with incomplete key security documents:

- The risk assessments [redacted] did not include all known system risks, and the Plan of Action and Milestones (POA&Ms) did not include all known control weaknesses or estimated completion dates for corrective action. For example:
  - [redacted]
    - [redacted]
    - [redacted]
  - [redacted]
    - [redacted]
    - [redacted]
    - [redacted]
  - [redacted]
    - [redacted]
    - [redacted]

NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013):

- Provides the structure for the security authorization of federal information systems, which includes:
  - Selecting and implementing security controls for the information system and describing how the controls are implemented in the SSP;
  - Assessing whether the controls are operating as intended;
  - Analyzing and assessing risk to the information system based on weaknesses and vulnerabilities identified;

- Documenting corrective action plans for known system weaknesses through the POA&M process; and

- Authorizing the information system to operate based on the determination of risk.

- Requires organizations to conduct an assessment of risk, 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.

- Requires agencies to assign a senior-level executive or manager as the authorizing official for the information system; ensure that the authorizing official authorizes the information system for processing before commencing operations; and update the security authorization at an organization defined frequency.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 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."

- Indicates: "The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions."

- Requires a POA&M to identify: "(i) the tasks to be accomplished with a recommendation for completion either before or after information system implementation; (ii) the resources required to accomplish the tasks; (iii) any milestones in meeting the tasks; and (iv) the scheduled completion dates for the milestones."

Until 2016, the NCUA included [redacted] within [redacted] authorization boundary; therefore [redacted] ATO covered these systems. In January 2016, the NCUA Chief Information Security Officer communicated to the system owners that [redacted] would no longer be included in [redacted] authorization boundary and would therefore require individual ATOs. In the latter part of 2016, the NCUA [redacted] and in December 2016, the authorizing official signed a new ATO, which no longer included these systems.

In January 2016, the Office of the Chief Information Officer (OCIO) began providing guidance and support to the system owners to complete the security assessment and authorization process for their systems. According to OCIO management, the efforts required to: (1) create or validate system development documentation; (2) identify system Points of Contact (POCs) due to the lack of Information System Security Officers (ISSOs) for each system; (3) develop the information security documentation; (4) train the system owners and POCs on the security authorization packages and signature requirements; and (5) conduct the security assessment and authorization activities exceeded the time OCIO management estimated it would take to conduct such activities. Therefore, the NCUA was unable to complete the system ATOs prior to the GSS authorization boundary change that occurred in December 2016.

In addition, OCIO management indicated the issues identified in the security authorization process for [redacted] were due to conducting security assessment and authorization activities for a large number of systems in a short timeframe with a limited number of knowledgeable resources (i.e., ISSOs). OCIO management informed us that the NCUA management approved a budget request to hire four ISSOs who will be responsible for managing the information security of the NCUA's portfolio of information systems, including the security authorization process.

In authorizing systems to operate, the authorizing official is accountable for accepting the risk(s) of operating these systems. Adequately documented risk assessments and POA&Ms provide the authorizing official the appropriate data necessary to make an informed decision on whether to authorize the system to operate considering the known vulnerabilities and risks (if applicable) and the estimated timeline to remediate any weaknesses in the systems. Ultimately, by properly authorizing systems to operate using all available information, the authorizing official is able to maintain the security posture of the NCUA information systems at an acceptable level of risk, decreasing the agency's exposure to compromised information or information systems.

We recommend that:

1. The Office of the Chief Information Officer ensure the NCUA maintains current authorizations to operate for all agency systems.

Agency Response:
Management concurred with the recommendation and indicated the NCUA finalized the update of its entire portfolio of legacy systems on October 27, 2017.

OIG Response:
We concur with management's actions taken. We received the finalized authorizations to operate after we completed fieldwork for the 2017 FISMA review and will assess them during the 2018 FISMA review.

2. The Office of the Chief Information Officer ensure the NCUA accomplishes security assessment and authorization activities in accordance with National Institute of Standards and Technology standards.

Agency Response:
Management concurred with the recommendation. Management indicated the Office of the Chief Information Officer is developing - by March 31, 2018 - a robust Independent Verification & Validation process to ensure assessment and authorization activities are maintained.

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

Enterprise Architecture Plan Incomplete

We determined the NCUA does not have a finalized Enterprise Architecture Plan. The NCUA's Enterprise Architecture Plan is currently in draft and addresses only the baseline ("As-Is") architecture; it does not take into account the Target ("To Be") architecture and the Sequencing Plan.

NIST SP 800-53, Revision 4, states organizations are to:

> Develop an enterprise architecture with consideration for information security and the resulting risk to organizational operations, organizational assets, individuals, other organizations, and the Nation.

NIST SP 800-39, *Managing Information Security Risk: Organization, Mission, and Information System View* (March 2011) states:

> Enterprise architecture is a management practice employed by organizations that establishes a clear and unambiguous connection from investments (including information security investments) to measurable performance improvements. It provides a disciplined and structured methodology for managing the complexity of the organization's information technology infrastructure.

The Common Approach to Federal Enterprise Architecture (May 2, 2012) (The Common Approach) provides guidance for the practice of Enterprise Architecture throughout the Executive Branch of the U.S. Federal Government. It "promotes increased levels of mission effectiveness by standardizing the development and use of architectures within and between Federal Agencies." It indicates:

- Enterprise Architecture includes a baseline architecture, a target architecture, and a sequencing plan.

- Baseline Architecture is the set of products that portray the existing enterprise, the current business practices, and technical infrastructure. It is commonly referred to as the "As-Is" architecture.

- Target Architecture is the representation of a desired future state or "to be built" for the enterprise within the context of the strategic direction.

The *Federal Enterprise Architecture Framework Version 2* (January 29, 2013) describes a suite of tools to help government planners implement The Common Approach. It indicates:

> The sequencing plan describes the as-is state, target state, and the integrated steps required to transition from the as-is to the target environment based on the identified recommendations.

The NCUA completed a first draft of the Enterprise Architecture Plan in October 2016. The agency is in the process of procuring a vendor to conduct an information technology modernization assessment. This assessment will include analysis of the "To Be" state of the NCUA enterprise architecture. Once completed, the NCUA Enterprise Architecture Plan will be updated and finalized.

Developing, documenting and implementing an enterprise architecture plan in accordance with federal standards will facilitate the alignment of the enterprise architecture with management's objectives. Information flow, system interfaces and system interoperability will be consistently managed across the enterprise. This will allow the NCUA to more efficiently, cost-effectively, and consistently manage risk and apply adequate protections to enable the agency to successfully meet its mission through its business functions.

We recommend that:

3. The NCUA complete the development and documentation of the Enterprise Architecture Plan in accordance with federal standards to include the Target or "To Be" architecture and the Sequencing Plan.

Agency Response:
Management concurred with the recommendation. Management indicated the NCUA will complete the first iteration of a comprehensive Enterprise Architecture and Sequencing Plan in accordance with applicable federal standards by September 30, 2018.

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

Agency Account Management Controls Not Always Enforced

We noted account management issues [redacted] NCUA systems as follows:

- [redacted]
  - The system did not automatically disable accounts [redacted] in accordance with the NCUA policy.
  - One of four accounts sampled from the total population of 17 accounts created during FY 2017 did not have evidence of access authorization.
- [redacted]
  - [redacted]
  - [redacted]
  - [redacted]
- [redacted]
  - System accounts were not [redacted] in accordance with the NCUA policy to validate the users' access was still appropriate based on job function.
- [redacted]
  - System accounts were not [redacted] in accordance with the NCUA policy to validate the users' access was still appropriate based on job function.
- [redacted]
  - [redacted]

Revision of Office of Management and Budget, Circular A-130, *Managing Information as a Strategic Resource*, (July 28, 2016), Appendix I (Responsibilities for Protecting and Managing Federal Information Resources), states agencies shall protect information in a manner commensurate with the risk that would result from unauthorized access, use, disclosure, disruption, modification, or destruction of such information.

NIST SP 800-53, Revision 4:

AC-2, *Account Management*, states organizations are to:

- Require approvals by organization-defined personnel or roles for requests to create information system accounts; and
- Review accounts for compliance with account management requirements at an organization-defined frequency.

AC-2, *Control Enhancement (3), Account Management/Disable Inactive Accounts,* states the organization is to automatically disable inactive accounts after an organization-defined time period.

AC-11, *Session Lock*, states organizations are to prevent further access to the system by initiating a session lock after an organization-defined time period of inactivity.

The *NCUA Information Security Procedural Manual*, May 23, 2017:

AC-2, *Account Management*, states the NCUA is to:

- Require approvals by program office-defined personnel for requests to create information system accounts.
- Automatically disable inactive accounts after 60 days or less of inactivity.
- Review accounts for compliance with account management requirements at least within every 365 days.

AC-11, *Session Lock*, requires a session lock after 15 minutes of inactivity be initiated for remote access connections.

Through December 15, 2016, [redacted] access management controls. OCIO management indicated that after the NCUA removed these systems from the [redacted] system

boundary effective December 2016, the system owners became responsible for account management controls for their own systems independent of [redacted] access controls. Systems owners have not fully developed and implemented their own account management controls for these systems. Specifically:

- Regarding inactive accounts:
  - The NCUA has not [redacted]
  - The NCUA has not [redacted] We discussed this with a manager [redacted] who explained the account management controls for the system. The manager indicated there are business needs [redacted] However, we reiterated the NCUA's requirement [redacted] in accordance with federal requirements and explained the security reasons for doing so as addressed below.
- Regarding account authorization, the NCUA:
  - Has not designed and implemented a process [redacted]
  - [redacted]
- The NCUA has not implemented a process for recertifying [redacted] accounts on a periodic basis to confirm users access remains appropriate based on job function.

[redacted]

Account management controls limit inappropriate access to information systems, protecting the NCUA's data from unauthorized modification, loss, and disclosure. For account management controls to be effective, they must be consistently implemented and monitored.

The NCUA [redacted] accounts to prevent users' access to the NCUA's network, which by design should prevent unauthorized access to the NCUA applications where the users' accounts are still active. [redacted] application accounts, system owners can reduce the risk(s) of dormant accounts being mishandled and misused to access sensitive application data.

In addition, [redacted] accounts at the application level in accordance with policy.

Furthermore, by ensuring that access requests are approved and by configuring the session lock setting in accordance with the NCUA policy, the NCUA can mitigate the risk of inappropriate or unauthorized access to its systems.

We recommend that:

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.

Agency Response:
Management concurred with the recommendation. Management indicated that by June 30, 2018, NCUA will: (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.

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

5. The Office of the Chief Information Officer configure the session lock setting in accordance with the NCUA policy.

Agency Response:
Management concurred with the recommendation and indicated the session lock settings for remote access will be consistent with NCUA policy by December 31, 2017.

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

External Information Systems' Agreements Not All Current

The NCUA did not keep information systems' agreements current [redacted] Specifically, we determined that the NCUA did not have a Memorandum of Understanding (MOU) or Interconnection Security Agreement (ISA) [redacted]

NIST SP 800-47, *Security Guide for Interconnecting Information Technology Systems*, (August 2002), specifies that an agreement should be documented for the interconnection between organizations. An MOU documents the terms and conditions for sharing data and information resources in a secure method. An ISA identifies the technical and security requirements for establishing, operating, and maintaining the interconnection and supports the MOU.

NIST SP 800-53, Revision 4, states organizations are to:

- Authorize connections from the information system to other information systems through the use of ISAs;
- Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and
- Review and update ISAs at an organization defined frequency.

The *NCUA Information Systems Procedural Manual*, CA-3, *System Interconnections*, states the NCUA is to:

- Authorize connections from the information system to other information systems through the use of ISAs or data sharing agreements;
- Document, for each interconnection, the interface characteristics, security requirements, and the nature of the information communicated; and.
- Review and, if necessary, update ISAs at least every year and whenever significant changes are implemented that could affect the security state of the information system, impacting the validity of the agreement.

OCIO management indicated that the lack of MOUs/ISAs [redacted] in the historical documentation has required ongoing activities to obtain the appropriate MOUs/ISAs [redacted] As a result, the parties did not execute the documents in accordance with NCUA policy.

By properly managing interfaces between the NCUA systems and external parties, through the use of MOUs and ISAs, the NCUA increases the likelihood that both parties are properly implementing controls for protecting data processing, storage, security, and transmission. Ultimately, this helps protect the confidentiality, integrity, and availability of the NCUA systems and data.

We recommend that:

6. The Office of the Chief Information Officer document and implement a validation process to confirm that all memorandums of understanding and interconnection security agreements are current.

Agency Response:
Management concurred with our recommendation. Management indicated NCUA will leverage its Independent Verification and Validation process by March 31, 2018 to ensure, among the other Assessment and Authorization artifacts, that the Memorandums of Understanding and Interconnection Security Agreements are current and accurate.

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

7. The Office of the Chief Information Officer ensure memorandums of understanding and interconnection security agreements are timely executed [redacted]

Agency Response:
Management concurred with our recommendation. Management indicated NCUA will leverage its Independent Verification and Validation process by March 31, 2018 to ensure, among the other Assessment and Authorization artifacts, that the Memorandums of Understanding and Interconnection Security Agreements are current and accurate.

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

Security Awareness Training Not Fully Completed

The NCUA did not ensure all individuals completed annual security awareness training. Specifically, we identified more than 150 individuals with NCUA network accounts that did not complete the training for this fiscal year.

NIST SP 800-53, Revision 4, requires agencies to provide basic security awareness training to information system users (including managers, senior executives, and contractors):

- As part of initial training for new users;
- When required by information system changes; and
- At an organization defined frequency thereafter.

The *NCUA Information Security Procedural Manual*, AT-2 *Security Awareness Training*, states the NCUA is to ensure all users, including managers, senior executives, and contractors complete basic information system security awareness training as part of initial training for new users, when required by system changes, and annually thereafter.

Office of the Chief Information Officer management did not validate that all network user accounts were included in the NCUA's Learning Management System, which notifies network users of the annual security awareness training requirement and tracks the completion status.

Requiring the NCUA system users to complete annual security awareness training helps refresh their understanding of key information security policies and practices for safely using the NCUA information systems and safeguarding sensitive agency and credit union information.

We recommend that:

8. The Office of the Chief Information Officer coordinate with the Office of Human Resources to ensure all the NCUA network users have a Learning Management System account in order to receive notification of the required security training.

Agency Response:
Management concurred with the recommendation. Management indicated the NCUA will validate all active network accounts are accurately synchronized, documented, and reflected in the Learning Management System directory to ensure receipt of required annual information security awareness training by October 31, 2018.

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

Appendix A: Unresolved Prior Year Recommendations

FISMA Report Fiscal Year	Recommendation	Management Planned Completion Date (per the Prior Year Report)
2016	1. NCUA assess the current process and alternative strategies [redacted]	December 31, 2018
2016	9. Configure [redacted]	March 31, 2018
2016	12. Implement a process to ensure NCUA tracks, tests, and approves [redacted]	December 31, 2017
2016	13. Complete the decommissioning [redacted] according to the schedule management specified.	March 31, 2018
2016	20. Enforce NCUA policy to ensure the agency appropriately and timely documents and updates POA&M items to reflect the current status on an ongoing basis, and the agency tests, validates, and documents corrective actions in order to close POA&Ms.	March 31, 2018
2016	23. OCIO update the NCUA GSS Contingency Plan to include the business impact analysis results addressing the recovery priorities of all critical agency mission/business processes and associated information systems.	December 31, 2018

Appendix B: 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.

During this review, we assessed the NCUA's information security program domains as identified in The Department of Homeland Security's FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (V1.0). 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 also assessed the NCUA's privacy management program.

We conducted our fieldwork from August 2017 through October 2017. 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 C: The NCUA Management Response

National Credit Union Administration
Office of the Executive Director

SENT VIA E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel

SUBJ: Management Response – FY 2017 Federal Information Security Modernization Act (FISMA) of 2014 Compliance

DATE: November 3, 2017

The following is our response to the recommendations set forth in the Office of Inspector General's draft report titled *FY 2017 Independent Evaluation of the NCUA's Compliance with FISMA*. We appreciate your recognition of our efforts to continue to strengthen our information security program. We concur with the report's recommendations.

OIG Report Recommendations #1 and #2

1. The Office of the Chief Information Officer (OCIO) ensures the NCUA maintains current authorizations to operate for all agency systems.

2. The OCIO ensures the NCUA accomplishes security assessment and authorization activities in accordance with National Institute of Standards and Technology standards.

Response: NCUA finalized the update of its entire portfolio of legacy systems on October 27, 2017. OCIO is developing a robust Independent Verification & Validation (IV&V) process to ensure assessment and authorization activities are maintained by March 31, 2018.

OIG Report Recommendation #3

3. The NCUA complete the development and documentation of the Enterprise Architecture Plan in accordance with federal standards to include the Target or "To Be" architecture and the Sequencing Plan.

Response: NCUA will complete the first iteration of a comprehensive Enterprise Architecture and Sequencing Plan in accordance with applicable federal standards by September 30, 2018.

OIG Report Recommendations #4 and #5

4. The NCUA System Owners, in coordination with the OCIO, 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.

5. The OCIO configure the session lock setting in accordance with the NCUA policy.

Response: NCUA will: (1) conduct a feasibility analysis for each legacy systems' 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 by June 30, 2018. In addition, the session lock settings for remote access will be consistent with NCUA policy by December 31, 2017.

OIG Report Recommendations #6 and #7

6. The OCIO document and implement a validation process to confirm that all memorandums of understanding and interconnection security agreements are current.

7. The OCIO ensures memorandums of understanding and interconnection security agreements are timely executed [redacted]

Response: NCUA will leverage its IV&V process by March 31, 2018 to ensure, among the other Assessment & Authorization artifacts, that the MOUs and ISAs are current and accurate.

OIG Report Recommendation #8

8. The OCIO will coordinate with the Office of Human Resources to ensure all the NCUA network users have a Learning Management System account in order to receive notification of the required security training.

Response: The NCUA will validate all active network accounts are accurately synchronized, documented, and reflected in LMS directory to ensure receipt of required annual information security awareness training by October 31, 2018.

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

Appendix D: Acronyms and Abbreviations

AIRES	Automated Integrated Regulatory Examination System
ALMS	Automated Liquidation Management Services
AO	Authorizing Official
ATO	Authority To Operate
CLA	CliftonLarsenAllen, LLP
CU	Credit Union
CUSO	Credit Union Service Organization
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
IIS	Insurance Information System
ISA	Interconnection Security Agreement
ISSO	Information Systems Security Officer
MOU	Memorandum of Understanding
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OIG	Office of Inspector General
OMB	Office of Management and Budget
POA&M	Plan Of Action and Milestones
POC	Point of Contact

Acronyms and Abbreviations (Continued)

SP	Special Publication
SSA	State Supervisory Authority
SSP	System Security Plan