NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

FY 2015 INDEPENDENT EVALUATION OF THE EFFECTIVENESS OF NCUA'S INFORMATION SECURITY PROGRAM UNDER THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

REPORT # OIG-15-10
NOVEMBER 13, 2015

James W. Hagen
Inspector General

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged CliftonLarsonAllen LLP (CLA) to independently evaluate the effectiveness of NCUA's information security program and practices as required by the Federal Information Security Modernization Act of 2014 (FISMA 2014) and to assess NCUA's privacy management program.

CLA evaluated NCUA's information security program and practices and its privacy management program through interviews, documentation reviews, technical configuration reviews and sample testing. CLA evaluated 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 addition, CLA conducted a vulnerability assessment of NCUA's information systems components.

In resolving prior year issues and recommendations, NCUA has continued to strengthen its information security program during Fiscal Year (FY) 2015. NCUA has also made progress in documenting its privacy program. NCUA does not have any repeat findings from prior years.

In addition to NCUA needing to continue to make improvements in its privacy management program, we identified three information security program areas in which NCUA needs to make improvements. We determined NCUA needs to make improvements in its risk management and configuration management programs and with its authentication controls. We made six recommendations, which would help NCUA continue to improve the effectiveness of its information security program and its privacy management program. We have included NCUA's comments in their entirety at Appendix A.

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

II. BACKGROUND

This section provides background information on the Federal Information Security Modernization Act (FISMA 2014) and the National Credit Union Administration (NCUA).

Federal Information Security Modernization Act

The President signed into law the E-Government Act (Public Law 107 347) on December 17, 2002, which includes Title III, Information Security (The Federal Information Security Management Act of 2002). The Federal Information Security Management Act of 2002 (FISMA) permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), 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 into law the Federal Information Security Modernization Act of 2014 (Public Law 113-283; FISMA 2014) amends Chapter 35 of 44 U.S.C. to provide reform to Federal information security. 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.

- Requires the OMB Director to, within one year of the enactment of FISMA 2014, revise Budget Circular A-130 to eliminate inefficient or wasteful reporting.

FISMA 2014 retains the requirement for Inspectors General to perform annual independent evaluations to determine the effectiveness of agency information security programs and practices.

The Department of Homeland Security (DHS) issued FY 2015 Inspector General FISMA Reporting Metrics on June 19, 2015 (version 1.2) to further empower OIGs to focus on how agencies are evaluating risk and prioritizing security issues. On October 30, 2015 OMB issued Fiscal Year 2015-2016 Guidance on Federal Information Security and Privacy Management

Requirement (M-16-03). This memorandum includes the requirements for FY 2015 Annual FISMA Reporting of metrics in accordance with FISMA 2104.

National Credit Union Administration (NCUA)

NCUA is the independent Federal agency that charters, supervises and insures the nation's Federal credit unions. NCUA insures many state-chartered credit unions as well. NCUA is funded by the credit unions it supervises and insures. 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.

NCUA strives to ensure that credit unions are empowered to make necessary business decisions to serve the diverse needs of their 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.

NCUA has a full-time three-member Board (NCUA Board) consisting of a chairman, a vice chairman and a member. The members of the Board are appointed by the President of the United States and confirmed by the Senate. 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 regularly meets in open session each month, with the exception of August, in Alexandria, Virginia.

III. OBJECTIVE

The audit objective was to perform an independent evaluation of NCUA information security and privacy management policies and procedures for compliance with FISMA 2014 and Federal regulations and standards. We evaluated NCUA's efforts related to:

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

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

IV. METHODOLOGY AND SCOPE

We evaluated 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, NIST standards and guidelines, the Privacy Act and OMB memoranda and information security and privacy policies.

During this audit, we assessed NCUA's information security program in the areas identified in The Department of Homeland Security's FY 2015 FISMA 2014 Reporting Metrics (V1.2). These areas included: Continuous Monitoring Management, Configuration Management, Identity and Access Management, Incident Response and Reporting, Risk Management, Security Training, Plan of Action and Milestones, Remote Access Management, Contingency Planning, and Contractor Systems. We also assessed NCUA's privacy management program.

We conducted our fieldwork from August 2015 through October 2015. We performed our audit in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient and 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.

V. 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- and privacy-related controls. NCUA addressed its prior year deficiencies and continues to make progress in documenting and implementing its privacy management program. In addition to its privacy management program, we identified three new information security areas pertaining to risk management program, configuration management program and its authentication controls that NCUA needs to improve. We discuss these issues below.

1. NCUA Needs to Improve its Risk Management Program

NCUA has not defined and communicated its organization-wide risk tolerance to those charged with implementing risk management at the information systems level.

NIST SP 800-39, Revision 1, *Managing Information Security Risk Organization, Mission, and Information System View* (March 2011) states: Effectively managing information security risk organization-wide requires key elements, including: ongoing recognition and understanding by senior leaders/executives of the information security risks to organizational operations and assets, individuals, other organizations, and the Nation arising from the operation and use of information systems; and establishing the organizational tolerance for risk and communicating the risk tolerance throughout the organization including guidance on how risk tolerance impacts ongoing decision-making activities.

NIST SP 800-53 Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, PM-9, Risk Management Strategy (April 2013), states that: Organizations are to develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations and the Nation associated with the operation and use of information systems; implement the risk management strategy consistently across the organization; and review and update the risk management strategy at a defined frequency or as required to address organizational changes. An organization-wide risk management strategy clearly communicates the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010) indicates that: An organization's risk executive (function) "helps to ensure: (i) risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its missions and business functions; and (ii) managing information system-related security risks is consistent across the

organization, reflects organizational risk tolerance, and is considered along with other organizational risks affecting mission/business success."

Although NCUA's Office of the Chief Information Officer (OCIO) documented and implemented a risk management strategy in 2014 that incorporated the assessment and evaluation of risks specific to the procurement and development of information systems, NCUA did not begin working on its overall organization-wide risk management strategy until late 2014. As a result, OCIO based its strategy to manage risk associated with the operation and use of the agency's information systems on a risk tolerance that it developed at the systems level rather than NCUA's organization-wide risk tolerance.

During 2015, NCUA implemented an agency level Enterprise Risk Management Council that reports quarterly to the Board of Directors. In addition, NCUA initiated an inventory of information collection activities via an information risk assessment survey to ascertain the agency's critical data, systems and applications, and self-identified risks. The outcome of the information collection activities will form the basis for the development of NCUA's risk registry and risk tolerance. Once NCUA establishes and communicates the agency's risk tolerance, OCIO will need to re-align the current information system risk tolerance with the organization-wide risk tolerance.

Documenting and communicating an organization-wide risk tolerance would enable OCIO to align its strategic goals, objectives and requirements for protecting its information and information systems with the risk tolerance that supports NCUA's mission and business success. Ultimately, this would help to ensure OCIO consistently manages and monitors information security-related risks related to the confidentiality, integrity and availability of agency and credit union information.

Recommendations:

We recommend that:

1. NCUA complete the process of assessing, documenting and communicating the organization-wide risk tolerance in accordance with NIST SP 800-37, Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems.

2. OCIO re-align its current information system risk tolerance with the organization-wide risk tolerance.

Agency Response:

NCUA concurred with both recommendations. Management indicated NCUA would complete the process of assessing, documenting, and communicating the organziation-wide risk tolerance by the end of the third quarter of 2016. Management also indicated OCIO would align

information system risk tolerance with the organization-wide risk tolerance by the end of the fourth quarter of 2016.

OIG Response:

We concur with management's planned actions.

2. NCUA Needs to Improve Its Authentication Controls

[redacted]

Recommendation:

We recommend that:

[redacted]

Agency Response:

[redacted]

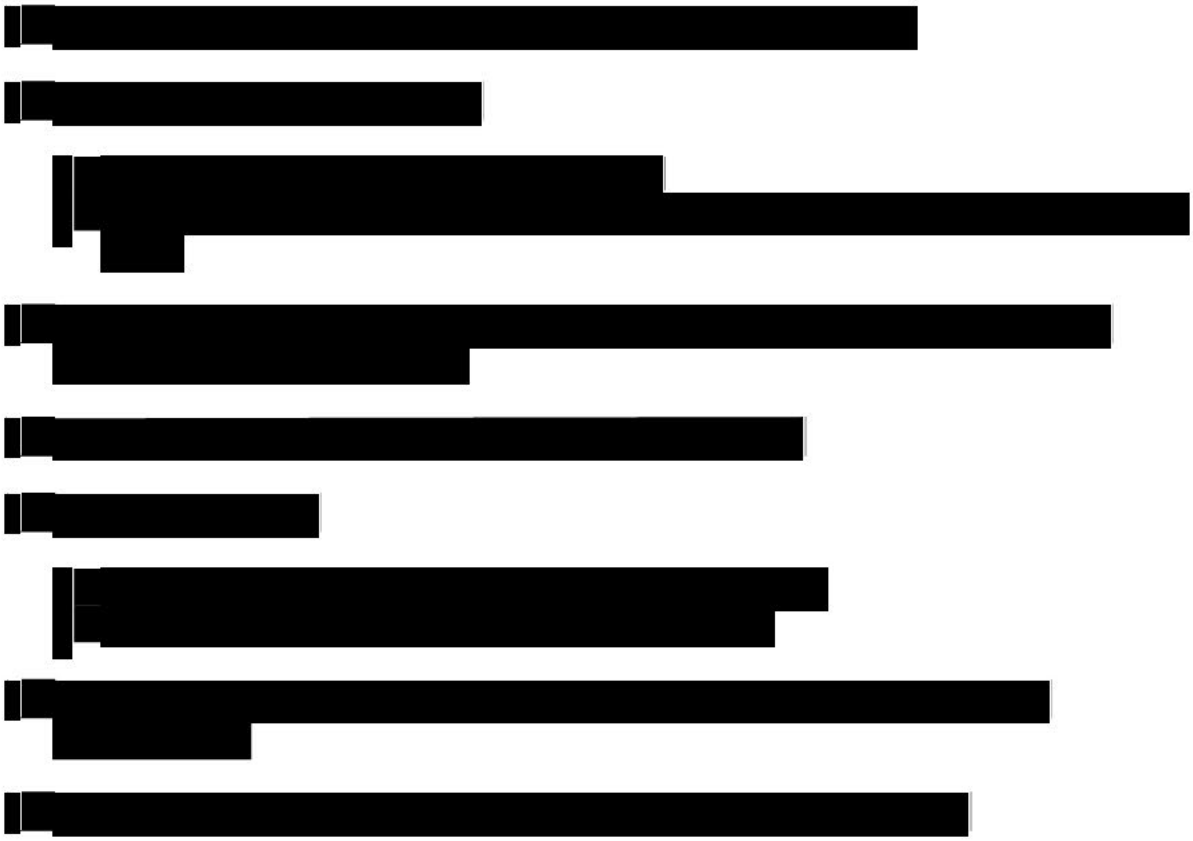
OIG Response:

We concur with management's planned actions.

3. NCUA Needs to Improve its Configuration Management Program

NCUA has information systems components within its infrastructure that the vendors no longer support. Although software vendors announce pending end of life/maintenance/support dates for

their products months or years in advance, NCUA did not take timely actions to plan for and implement newer versions prior to the end of vendor support. Following are those components and when the vendor stopped providing support (if available):



NIST Special Publication 800-53, Revision 4, Security and Privacy Controls for Federal Information Systems and Organizations, requires organizations to install security-relevant software and firmware updates on an organization-defined time period following the release of the updates. Organizations are to identify information systems affected by announced software flaws including potential vulnerabilities resulting from those flaws, and report this information to designated organizational personnel with information security responsibilities. Security-relevant software updates include, for example, patches, service packs, hot fixes, and anti-virus signatures.

NIST Special Publication 800-53, Revision 4 also requires organizations to replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer. Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

By replacing unsupported software and components within its infrastructure in a timely manner, NCUA will have reasonable assurance that: (1) its systems are not susceptible to old vulnerabilities and exploits that the vendors have addressed with current supported versions; and (2) it will receive continued support from the vendors against future vulnerabilities and exploits. Ultimately, NCUA will - on a continuous basis - more effectively protect its infrastructure and sensitive NCUA and credit union information against potential compromise.

Recommendation:

We recommend that:

4. OCIO complete the migration of its unsupported applications from their existing platform to platforms that are vendor-supported.

Agency Response:

NCUA concurred with this recommendation. Management indicated its estimated schedule to resolve the migration to vendor-supported platforms is the end of the fourth quarter 2016. In addition, management pointed out that many of the conditions for the information system components identified in the report are in legacy systems that OCIO has targeted for replacement or modernization.

OIG Response:

We concur with management's planned actions.

4. NCUA needs to Improve its Privacy Program

Although NCUA has established a Privacy Program that provides the general framework for addressing privacy requirements, the agency has not fully implemented its Privacy Program. Specifically:

- NCUA's existing privacy policies and procedures do not comprehensively address protecting and ensuring the proper handling of personally identifiable information (PII);
- NCUA has not fully documented controls associated with NCUA privacy policies and procedures for all programs, information systems, and technologies involving PII; and
- NCUA has not fully updated its General Support System Security Plan to address current NIST privacy controls.

NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010) states organizations are to develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and where appropriate, at the system level.

NIST 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations* (April 2013), AR-1 Governance and Privacy Program states organizations are to develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), in consultation with legal counsel, information security officials, and others as appropriate, ensures the development, implementation, and enforcement of privacy policies and procedures.

In addition NIST 800-53, Revision 4 provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form. The controls

focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary. The privacy families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership and oversight of the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and in coordination with the Chief Information Security Officer, Chief Information Officer, program officials, legal counsel, and others as appropriate.

NIST 800-53, Revision 4 also states the system security plan is to describe the controls in place or planned.

NCUA has not assigned dedicated resources to develop and implement the agency's Privacy Program. The two attorneys NCUA has assigned to oversee the Privacy Program have other responsibilities within the Office of the General Counsel. While they have made progress in documenting the general framework of NCUA's Privacy Program, management believes additional resources would be helpful in order to document the privacy policies and procedures and associated controls necessary to fully implement and support the privacy program.

The purpose of a fully and formally documented Privacy Program is to define the agency-wide privacy policies and practices. Implementing comprehensive privacy policies and procedures mitigates the likelihood that NCUA staff members will not fully address privacy throughout the lifecycle of the agency's information systems. In addition, formal privacy policies and procedures will provide employees and contractors with consistent and comprehensive guidance to adequately handle and protect agency and credit union PII. Furthermore, these policies and procedures will facilitate accountability in effectively administering the implementation and management of the agency's Privacy Program. Consequently, these formal policies and procedures will help NCUA ensure proper handling of PII, ultimately mitigating the potential for personal harm, loss of public trust, or increased costs associated with inappropriate or unauthorized access to PII.

Recommendations:

We recommend that:

5. The Senior Agency Official for Privacy complete the documentation and implementation of the privacy policies and procedures and associated controls to support and monitor the organization-wide Privacy Program in accordance with NIST guidance.

6. OCIO update the General Support System Security Plan to include the control implementation descriptions for NIST privacy controls once NCUA documents and

disseminates the organization-wide privacy policies and procedures and associated controls.

Agency Response:

Management concurred with the recommendations and indicated the Senior Agency Official for Privacy will document and implement the privacy policies and procedures and associated controls by the end of the fourth quarter 2016. Management also indicated that OCIO will update the General Support System Security Plan by the end of the first quarter 2017.

OIG Response:

We concur with management's planned actions.

Appendix A: NCUA Management Response

National Credit Union Administration
Office of the Executive Director

SENT BY EMAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel

SUBJ: Compliance with the Federal Information Security Modernization Act

DATE: November 10, 2015

The following is our response to the recommendations set forth in the Office of Inspector General's report titled *Compliance with the Federal Information Security Modernization Act.* We concur with the report recommendations. Below are more detailed responses to each of the recommendations.

OIG Report Recommendations #1 and #2

1. NCUA complete the process of assessing, documenting, and communicating the organization-wide risk tolerance in accordance with NIST SP 800-37, Revision 1 Guide for Applying the Risk Management Framework to Federal Information Systems.

2. OCIO re-align its current information system risk tolerance with the organization-wide risk tolerance.

Response to Recommendations 1 and 2: NCUA concurs with both recommendations and will complete the process of assessing, documenting, and communicating the organization-wide risk tolerance by the end of Q3 2016. By the end of Q4 2016, OCIO will align the information system risk tolerance with the organization-wide risk tolerance as needed.

OIG Report Recommendation #3

[redacted]

Response: [redacted]

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

OIG Report Recommendation #4

4. OCIO complete the migration of its unsupported applications from their existing platform to platforms that are vendor-supported.

Response: NCUA concurs with the recommendation. Many of the conditions identified for the referenced information system components exist today in legacy systems that are targeted for replacement or modernization. The estimated schedule to migrate to vendor-supported platforms show all being resolved by the end of Q4 2016.

OIG Report Recommendations #5 and #6

5. The Senior Agency Official for Privacy complete the documentation and implementation of the privacy policies and procedures and associated controls to support and monitor the organization-wide Privacy Program in accordance with NIST guidance.

6. OCIO update the General Support System Security Plan to include the control implementation descriptions for NIST privacy controls once NCUA documents and disseminates the organization-wide privacy policies and procedures and associated controls.

Response to Recommendations 5 and 6: NCUA concurs with the recommendations and will complete the documentation and implementation of the privacy policies and procedures and associated controls in accordance with NIST guidance by the end of Q4 2016. By the end of Q1 2017, OCIO will update the General Support System Security Plan to include the control implementation descriptions for NIST privacy controls once NCUA documents and disseminates the organization-wide privacy policies and procedures and associated controls.

Thank you for the opportunity to review and comment on the report. If you have any questions, please do not hesitate to contact my office.

cc: Deputy Executive Director Kutchey
Chief Information Officer Dorris
Associate General Counsel Dent

Appendix B: Acronyms and Abbreviations

AMAC	Asset Management and Assistance Center
CLA	CliftonLarsenAllen, LLP
CPO	Chief Privacy Officer
CU Online	Credit Union Online Call Report System
DHS	Department of Homeland Security
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act of 2014
HSPD	Homeland Security Presidential Directive
ID	Identification
IDS	Intrusion Detection System
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
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan Of Action and Milestones
SAOP	Senior Agency Official for Privacy
VPN	Virtual Private Network