NATIONAL CREDIT UNION ADMINISTRATION

OFFICE OF INSPECTOR GENERAL

INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 2014

REPORT # OIG-14-08
NOVEMBER 12, 2014

James W. Hagen
Inspector General

W. Marvin Stith, CISA, CICA
Sr. Information Technology Auditor

TABLE OF CONTENTS

Section **Page**

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged CliftonLarsonAllen LLP (CLA) to independently evaluate NCUA's information systems and information security program and controls for compliance with the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002.

CLA evaluated NCUA's information security 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, 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 resolving prior year issues and recommendations, NCUA has continued to strengthen its information security program during Fiscal Year (FY) 2014. NCUA is also continuing to make progress in documenting its privacy program, which the agency indicated it is on track to complete by June 2015. Therefore, we are not including this open issue and recommendation this year. NCUA does not have any repeat findings from prior years.

This year we identified two findings in the areas of NCUA's configuration management program and oversight of its contractor systems. We made three recommendations, which would help NCUA continue to improve its information security program. NCUA agreed with all the recommendations. 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 Management Act (FISMA) and the National Credit Union Administration (NCUA).

Federal Information Security Management Act

The President signed into law the E-Government Act (Public Law 107 347), which includes Title III, Information Security, on December 17, 2002. The Federal Information Security Management Act (FISMA) permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues the annual review and reporting requirements introduced in GISRA. In addition, it includes new provisions aimed at further strengthening the security of the Federal government's information and information systems, such as development of minimum standards for agency systems. In general, FISMA:

- Lays out a framework for annual information technology security reviews, reporting, and remediation plans.
- Codifies existing OMB security policies, including those specified in Circular A-130, Management of Federal Information Resources, and Appendix III.
- Reiterates security responsibilities outlined in the Computer Security Act of 1987, Paperwork Reduction Act of 1995, and Clinger-Cohen Act of 1996.
- Tasks NIST with defining required security standards and controls for Federal information systems.

The Department of Homeland Security (DHS) issued the FY 2014 reporting metrics, which provide measures against which agency Chief Information Officers, Offices of Inspector General, and Senior Agency Officials for Privacy assess the status and compliance of agencies' information security and privacy management programs. On October 3, 2014 OMB issued Fiscal Year 2014-2015 Guidance on Improving Federal Information Security and Privacy Management Practices (M-15-01). This memorandum includes the reporting requirements for FY 2014 Reports to OMB and Congress in accordance with Section 301 § 3544 of FISMA.

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 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.

NCUA has a full-time three-member Board (NCUA Board) consisting of a chairman and two members. 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 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; and
- Remediating prior audit weaknesses pertaining to FISMA 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, 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 2014 Inspector General FISMA Reporting Metrics.

These areas included: continuous monitoring management, configuration management, identity and access management, incident response and reporting, risk management, security training, POA&M, remote access management, contingency planning, contractor systems, and security capital planning. We also assessed NCUA's privacy management program.

We conducted our fieldwork from August 2014 through October 2014. 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 has made significant progress in addressing prior year reported deficiencies. We also determined NCUA is continuing to make progress in documenting its privacy program, which the agency indicated it is on track to complete by June 2015. Therefore, we are not including this issue or recommendation this year. We identified two new issues pertaining to NCUA's oversight of contractor systems and its configuration management. We discuss these issues below.

1. NCUA needs to improve its Configuration Management Program

NCUA addressed the configuration management issues from the FY 2013 FISMA review, including documenting a comprehensive program. This year, we also assessed a sample of NCUA's security configuration settings and noted the following settings were not configured in compliance with United States Government Configuration Baseline (USGCB)[1] standards for the NCUA network:

- The USGCB standard for the account lockout group policy is 5 logon attempts. NCUA's was configured to 10 attempts;
- The USGCB standard for password history is 24 passwords remembered. NCUA's was configured to 5 passwords remembered; and
- The USGCB standard for password length is 12 characters. NCUA's was configured to 8 characters.

The Federal Information Security Management Act (FISMA) (Section 3544(b)(2)(D)(iii)) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Common security configurations provide a baseline level of security, reduce risk from security threats and vulnerabilities, and save time and resources.

In addition, OMB M-11-33, FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management states in FY 2010, the CIO Council announced the creation of the United States Government Configuration Baselines (USGCB) which is maintained by the CIO Council's Technology Infrastructure Subcommittee. USGCB is intended to be the core set of security related configuration settings with which all federal agencies should comply. Agencies should make risk based decisions as they customize the

[1] USGCB is a federal government-wide initiative that provides guidance to agencies on what should be done to improve and maintain effective configuration settings, focusing primarily on security.

baseline for their operational environment and should document and track any changes, including implementation of more secure settings.

Furthermore, NIST 800-39, Managing Information Security Risk, Organization, Mission, and Information System View, indicates that risk acceptance is the appropriate risk response when the identified risk is within the organizational risk tolerance. Organizations can accept risk deemed to be low, moderate, or high depending on particular situations or conditions. Conversely, organizations may accept substantially greater risk (in the moderate/high range) due to compelling mission, business, or operational needs.

NCUA documented its rationale for accepting the risk of not implementing the required network authentication settings. The agency indicates it is due to resistance from its work force in the field who believe that the more secure settings would create an undue burden and adversely impact productivity. NCUA has not alternatively determined a compelling mission, business or operational need for non-compliance with the USGCB settings.

Considering NCUA relies on single-factor authentication for logical access to its network, it is especially critical that NCUA enforce required USGCB authentication controls to help mitigate the potential for brute force password guessing and the vulnerabilities associated with frequent reuse of weak or compromised passwords.[2] Ultimately, these stronger USGCB security controls help mitigate the potential for unauthorized modification, loss or disclosure of NCUA information and resources.

Recommendations: We recommend that the NCUA Chief Information Officer:

1. Document and implement policies requiring stronger authentication controls that are in compliance with USGCB requirements.

Agency Response:

OCIO will work with impacted stakeholders to strengthen configuration settings as part of the new laptop rollout, scheduled to be completed May 31, 2015.

OIG Response: The OIG Concurs.

[2] NCUA has appropriately established and documented operational and business needs for not implementing NIST-required two-factor authentication for logical access to the NCUA network.

2. NCUA needs to improve Oversight of its Contractor Systems

NCUA did not always formally or adequately assess or document residual security risks to the agency from contractor systems before allowing these systems to operate within the NCUA environment. Specifically:

- NCUA did not review the Authorization to Operate (ATO) and supporting documentation including the System Security Plan, Risk Assessment and Plan of Action and Milestones for the CyberGrants and MobileIron contractor systems.

- The ATO for the Learning Management System (LMS) states an Interim Authority to Operate was issued prior to completing the full security assessment and authorization activities required by NIST. However, NCUA did not formally document the residual risk to the Agency.

- The ATO for Pay.gov states residual risk was documented in the contractor's POA&Ms and/or Risk Acceptance Memo. However, NCUA did not review the POA&Ms or Risk Acceptance Memo to assess residual risk to the NCUA.

NIST 800-37, Guide for Applying the Risk Management Framework to Federal Information Systems, A Security Life Cycle Approach states the risk management framework emphasizes maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to the organization arising from the operation and use of information systems. FISMA and OMB policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies. These security requirements also apply to external subsystems storing, processing, or transmitting federal information and any services provided by or associated with the subsystem. The assurance or confidence that the risk from using external services is at an acceptable level depends on the trust that the organization places in the external service provider. When the level of trust in the external provider of subsystems/services is below expectations, the organization: (i) employs compensating controls; (ii) accepts a greater degree of risk; or (iii) does not obtain the service (i.e., performs its core missions and business operations with reduced levels of functionality or possibly no functionality at all).

NCUA completed the formal documentation of its new risk management procedures related to contractor oversight effective September 29, 2014. These new procedures address monitoring for up-to-date security documentation and performing risk reviews that NCUA had not consistently performed in the past. NCUA indicated it will implement these new procedures to improve oversight of contractor systems. As a result, these new procedures should help facilitate NCUA in adequately evaluating and documenting risks from contractor systems. Ultimately, assessing the risks will help NCUA implement any necessary compensating controls to protect the storage, processing, or transmission of agency information.

Recommendations: We recommend that NCUA management:

2. Fully implement its Contractor System Oversight Procedures to include formally assessing and documenting residual risk to the agency from contractor systems on an ongoing basis.

3. Ensure compensating controls are documented and implemented when security controls for contractor systems are not at an acceptable level.

Agency Response:

OCIO documented NCUA's Contractor Systems Oversight Procedure. The new process will assess and document risk and compensating controls for all new contractor systems on an ongoing basis effective October 1, 2014. OCIO will assess and document risk and compensating controls of the systems identified in the report by March 31, 2015.

OIG Response: The OIG Concurs.

VI. Appendix A: NCUA Management Response

National Credit Union Administration

Executive Director

OCIO/DC
SSIC 13500

SENT BY E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel

SUBJ: Independent Evaluation of the NCUA's Compliance with the Federal Information Security Management Act (FISMA) 2014

DATE: November 7, 2014

This memorandum responds to your request for comment on the Independent Evaluation of the NCUA's Compliance with the Federal Information Security Management Act (FISMA) 2014. Thank you for the opportunity to review and comment on your report's findings and recommendations. We concur with all recommendations. Below is an outline of our plan of action from the Office of the Chief Information Officer (OCIO).

Recommendation 1: Document and implement policies requiring stronger authentication controls that are in compliance with USGCB requirements.

Response: OCIO will work with impacted stakeholders to strengthen configuration settings as part of the new laptop rollout, scheduled to be completed May 31, 2015.

Recommendation 2: Fully implement its Contractor System Oversight Procedures to include formally assessing and documenting residual risk to the agency from contractor systems on an ongoing basis.

Recommendation 3: Ensure compensating controls are documented and implemented when security controls for contractor systems are not at an acceptable level.

Response to Recommendations 2 and 3: OCIO documented NCUA's Contractor Systems Oversight Procedure. The new process will assess and document risk and compensating controls for all new contractor systems on an ongoing basis effective October 1, 2014. OCIO will assess and document risk and compensating controls of the systems identified in the report by March 31, 2015.

Thank you for the opportunity to respond and please do not hesitate to contact my office if you need anything further.

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