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) 2013

Report # OIG-13-12
November 22, 2013

James Hagen
Inspector General

Released by:

W. Marvin Stith, CISA
Sr. Information Technology Auditor

Table of Contents

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged Mitchell & Titus, LLP (Mitchell & Titus)[1] to independently evaluate NCUA's information systems and security program and controls for compliance with the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002.

Mitchell & Titus evaluated NCUA's security program through interviews, documentation reviews, technical configuration reviews, and sample testing. Mitchell & Titus 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 security and privacy policies.

NCUA has worked to significantly strengthen its information security and privacy programs during Fiscal Year (FY) 2013. We believe that many of the improvements within the agency's information security program are the result of the acquisition of additional dedicated resources within the Office of the Chief Information Officer to address information security issues. However, while NCUA continues to make improvements in the following areas, we identified remaining issues in these areas from last year's FISMA review that NCUA officials need to address:

- Finalizing its Continuous Monitoring Policies, Procedures, and Strategy;
- Finalizing its Risk Management Policies and Procedures;
- Improving its Configuration Management Program;
- Improving its New Hire Security Awareness Training Program; and
- Improving Oversight and Management of its Contractor Systems.

In addition, we identified a new finding pertaining to NCUA's remote access program. We made nine recommendations in these areas, which would help NCUA continue to improve its information security program. Furthermore, we conducted a vulnerability assessment of NCUA's network components this year. NCUA had very few findings from this assessment. We will provide the results separately to NCUA for review, response and corrective action.

We appreciate the courtesies and cooperation provided to our staff and Mitchell & Titus staff during this audit.

[1] Mitchell & Titus, LLP is a member firm of Ernst & Young Global Limited.

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; and

- Tasks NIST with defining required security standards and controls for Federal information systems.

The Department of Homeland Security (DHS) issued the FY 2013 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.[2] On November 18, 2013 OMB issued the Fiscal Year (FY) 2013 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management. This document provides instructions for meeting agencies' FY 2013 reporting requirements under FISMA. It also includes reporting instructions on agencies' privacy management programs. Furthermore, it includes the requirement for Chief Information Officers of CIO Council member agencies to submit monthly data feeds.

[2] DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cyber security with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543.

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 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 security and privacy policies.

During this audit, we assessed NCUA information security and privacy management programs in the areas identified in The Department of Homeland Security's FY 2013 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. In addition, we conducted a vulnerability assessment of NCUA's network components.

We conducted our fieldwork from July 2013 through November 2013. 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 last year's reported deficiencies; however, some prior year deficiencies remain. In addition, we identified a new deficiency in the area of remote access that requires management's attention. Below we discuss the issues that remain from the prior year and the remote access issue.

This year, we also conducted a vulnerability assessment of NCUA's network components. NCUA had very few findings from this assessment. We will provide the results separately to NCUA for review, response, and corrective action. We note that NCUA immediately remediated some of the issues from the vulnerability assessment.

1. NCUA needs to improve its Continuous Monitoring Program

While NCUA has continued to improve its continuous monitoring program and has many of the components with which to build a robust program, NCUA has not finalized its policies and procedures. In addition, it has not fully integrated the various components of its information security program into a strategy that facilitates near real-time monitoring and risk management. This finding includes issues in the following areas that we address in other sections of the report:

- Risk management policies and procedures (see page 6);
- Configuration management of Macintosh computers(see page 7); and
- Oversight of contractor systems (see page 11).

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2009 with updates as of May 1, 2010), guides that agencies should establish a continuous monitoring strategy and implement a continuous monitoring program that includes: A configuration management process for the information system and its constituent components; a determination of the security impact of changes to the information system and environment of operation; ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and reporting the security state of the information system to appropriate organizational officials.

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), guides that Information Security Continuous Monitoring (ISCM) supports agency risk management decisions e.g., risk response decisions, ongoing system authorization decisions, Plans of Action and Milestones (POA&M) resource and prioritization decisions, etc. It also indicates that maintaining an up-to-date view of information security risks across an organization requires the involvement of the entire agency, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual information systems in support of the organization's core missions and business functions.

NIST SP-800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010), guides that a robust continuous monitoring program requires the active involvement of information system owners and common control providers, chief information officers, senior information security officers, and authorizing officials. The monitoring program allows an organization to: track the security state of an information system on a continuous basis; and maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

NCUA indicated it did not have dedicated information security resources until late in the year to work on completing the documentation of its Continuous Monitoring policies and procedures and to establish a comprehensive strategy that covers all components of its continuous monitoring Program.

By improving and implementing a comprehensive continuous monitoring program, NCUA will be more aware of and better prepared to respond to potential threats and vulnerabilities. Ultimately, NCUA will be able to better protect the confidentiality, integrity, and availability of its systems and data.

Recommendation: We recommend that NCUA management:

1. Complete the documentation and implementation of comprehensive continuous monitoring strategies, policies and procedures in accordance with guidance under Information Security Continuous Monitoring, the Risk Management Framework and other NIST guidance.

Agency Response:

OCIO plans to complete the documentation and implementation of its Continuous Monitoring program by December 31, 2014.

OIG Response: The OIG Concurs.

2. NCUA needs to improve its Risk Management Program

NCUA has made significant progress since FY 2012 in implementing a comprehensive risk management program. Specifically, NCUA addressed most of the deficiencies in this area from last year and has drafted its Risk Management Framework policies and procedures in its Information System Security Policy and Procedure Handbook (System Security Handbook). However, NCUA is still in the process of finalizing the System Security Handbook.

The Risk Management Framework - as prescribed by NIST SP 800-37 - is the foundation for implementing and maintaining an effective information security program. NIST SP 800-37 provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

In response to the FY 2012 FISMA evaluation, NCUA indicated it would address all the issues we identified with its Risk Management program by July 2013. While NCUA addressed the majority of the issues and was able to draft its Risk Management policies and procedures, it did not have sufficient resources to finalize the Security Handbook by the stated completion date.

When NCUA finalizes its Risk Management policies and procedures, it will have formally established its procedures to more adequately manage its information systems-related risks and protect its data and information systems consistent with the Risk Management Framework.

Recommendation: We recommend that NCUA management:

2. Finalize its Information System Security Policy and Procedure Handbook.

Agency Response:

OCIO will finalize the current draft Information System Security Policy and Procedure Handbook by September 30, 2014.

OIG Response: The OIG Concurs.

3. NCUA needs to improve its Configuration Management Program

While NCUA has continued to make improvements with its configuration management program, NCUA does not have adequate configuration management policies and procedures. Specifically:

- NCUA's configuration management policies and procedures do not adequately address purpose, scope, roles and responsibilities; management commitment; coordination among organizational entities necessary to control and manage configurations; and the timely processing of remediated configurations.

- For part of the calendar year, NCUA did not require or enforce that comments be included when testing Change Control Requests (CCRs). As a result, NCUA did not document testing evidence for most of the 117 CCRs addressed during that period. NCUA implemented corrective action for this area in June 2013; therefore, we will not make a recommendation to address this issue.

- NCUA does not have a documented configuration baseline for its two Macintosh computers and does not have a process in place to monitor and update critical security patches for these computers.

NIST SP 800-53, Revision 3, guides that organizations should develop, disseminate, and review/update a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

FIPS PUB 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006), requires agencies to establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and establish and enforce security configuration settings for information technology products employed in organizational information systems. FIPS PUB 200 also requires agencies to identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response.

NCUA indicated it did not have information security resources dedicated until late in the year to adequately document policies and procedures and to establish a comprehensive program that covers all of the systems and devices within the NCUA environment.

By documenting and establishing a comprehensive configuration management program, NCUA can more effectively and efficiently monitor, manage, and patch the security configurations for all systems and devices within the NCUA information system environment. Ultimately, a more comprehensive program will help ensure NCUA protects the confidentiality, integrity and availability of all the agency's systems and data.

Recommendations: We recommend that NCUA management:

3. Document a comprehensive configuration management program that includes policy and procedures for monitoring, managing, and patching security configurations for all systems and devices.

   Agency Response:

   OCIO will finalize documentation of its Configuration Management program by September 30, 2014.

4. Establish and implement a baseline configuration for the Macintosh computer(s).

   Agency Response:

   OCIO plans to document its Macintosh computer baseline by September 30, 2014.

OIG Response: The OIG Concurs with management's responses.

4. NCUA needs to improve Remote Access Controls

While NCUA indicated it allows short-term contractors[3] to remotely access its network, NCUA does not require these contractors to use two-factor authentication.

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), requires that agencies allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access. In addition, NIST SP 800-118, Guide to Enterprise Password Management (Draft, April 2009) indicates that using more than one factor for authentication makes it more difficult for someone to gain unauthorized access to a system. For example, it is easier to either discover a user's password or steal the user's smart card than it is to both steal the smart card and also discover the user's password. Furthermore, NIST SP 800-53 guidance indicates that authenticating user identities for multifactor authentication is accomplished through some combination of passwords, tokens, or biometrics.

In accordance with federal requirements[4], NCUA requires [long-term] contractors scheduled to work at NCUA for more than 180 days to use PIV cards for access to federal facilities and information systems. The PIV cards provide for two-factor

[3] Short-term contractors are contractors scheduled to work at the agency for 180 days or less.

[4] Homeland Security Presidential Directive-12 (August 27, 2004) mandates the issuance of electronic identity credentials to Federal employees and contractors. OMB M-05-24 (August 5, 2005) clarified the eligibility requirements for PIV Cards to temporary Federal employees and contractors, by requiring PIV Card issuance to all Federal employees and contractors who require access to Federal facilities or information systems for more than six months.

authentication for long-term employees and contractors to remotely access the NCUA network. For short-term contractors who remotely access the network, NCUA's policy indicates:

> Short-term contractors do not use PIV; however, compensating controls include the following: 1) Remote login requires the contractor to use an NCUA issued laptop which checks for certificates on the machine from the NCUA Certificate Authority, and 2) Remote login also requires unique credentials for the user to login with the NCUA laptop.

NCUA indicated it has accepted the risk of *not* requiring two-factor authentication for short-term contractors. However, we reiterate that as indicated in federal requirements and guidance, the two-factor authentication requirement provides for a stronger control than one factor authentication, and the requirement is not optional based on the term of the contract work.

By implementing two-factor authentication for remote access by short-term contractors, NCUA would be able to best protect its systems and data from the risk of unauthorized access.

Recommendations: We recommend that NCUA management:

5. Initiate an assessment involving representatives from each of the responsible directorates to determine an appropriate two-factor authentication plan, process and mechanism for short-term contractors to remotely access the NCUA network.

   Agency Response:

   OCIO will perform a formal risk assessment of Remote Access solutions for short-term contractors by June 30, 2014.

6. Develop, document and implement two-factor authentication of short-term contractors who access the NCUA network remotely.

   Agency Response:

   OCIO will finalize its Remote Access policies for short-term contractors by June 30, 2014.

OIG Response: The OIG Concurs with management's responses.

5. NCUA needs to improve its Security Awareness Training Program

We determined NCUA's procedures for providing security awareness training to new hires are not adequate. Specifically, NCUA:

- Has not established a specific timeframe within which new hires must complete the agency's initial security awareness training.
- Does not retain evidence indicating that new hires have completed their initial security awareness training.
- Does not have documented procedures to monitor and review the timely completion of security awareness training by new hires and to enforce sanctions for not completing the training.

NIST SP 800-53 guides that organizations should:

- Provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and periodically thereafter;
- Document and monitor individual information system security training activities including basic security awareness training; and
- Retain individual training records for a specific period of time as defined by the organization.

NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (April 1998), requires training: for new employees within 60 days of hire.

During the FY 2012 FISMA review, NCUA indicated it did not have the dedicated resources until late in the year to develop, document, implement and monitor a robust security awareness training program that meets NIST guidance and requirements. This year NCUA indicated it just recently assigned the dedicated resources to address its security awareness training program.

By implementing a current and effective security awareness training program, NCUA management can help ensure all personnel receive the required security training and in a timely manner. Individuals who receive adequate and current security training and who are aware of their security responsibilities will be better prepared to perform their assigned duties in the most secure manner. Ultimately, this helps protect the confidentially, availability, and integrity of NCUA systems and data.

Recommendation: We recommend that NCUA:

7. Develop and document a new hire security awareness training program that provides for:

   a. Monitoring, tracking, and reviewing the timely completion of new hire training; and

   b. Enforcing sanctions for not completing security awareness training within the required time-frame.

Agency Response:

OCIO will update the new hire training process and procedures and address enforcement of sanctions by March 31, 2014.

OIG Response: The OIG Concurs with management's response.

6. NCUA needs to improve Oversight of its Contractor Systems

NCUA has not fully implemented a formal contractor system oversight management process in alignment with current federal guidelines. Specifically:

- Current NCUA policies and procedures do not provide sufficient guidance in regards to how NCUA should monitor and assess information security requirements for its contractor systems. As a result, NCUA does not have a formal process in place:
  - For maintaining sufficient assurance that security controls of contractor provided or hosted systems and services are effectively implemented and comply with federal and NCUA guidelines;
  - To ensure it obtains the System Security Plans (SSPs) of contractor systems. Specifically, NCUA does not have the SSPs for any of its eight (8) contractor systems; and
  - For classifying contractor systems as FISMA-reportable systems and cloud systems within its system inventory.
- For the six of its eight (8) contractor systems, NCUA either (a) did not receive the Memorandums of Understanding or Interconnection Security Agreements (MOU/ISA) necessary to review and monitor the service agreement; or (b) the

SOC 1 (Service Organizations Control) reports[5] NCUA received did not include adequate security information as indicated by NIST guidance:

- Not all the NCUA functional owners of the contractor systems are identified.

NIST SP 800-53 guides that organizations develop and maintain an inventory of its information systems. In addition, NIST SP 800-53 guides that organizations authorize connections from their information systems to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements, and document - for each connection - the interface characteristics, security requirements and the nature of the information communicated; and monitor the interconnections on an ongoing basis to verify enforcement of security requirements.

OCIO is centrally responsible for the security of all systems operating in the NCUA environment. However, functional system owners - who are responsible for obtaining and maintaining the security documentation for contractor systems - do not always consult with or seek approval from OCIO regarding appropriate security documentation. Therefore, NCUA management has not been able to effectively monitor all contractor systems and ensure compliance of these systems with Federal and NCUA information security requirements.

By centrally managing its contractor oversight process, NCUA can have better assurance that contractor systems operating in or connected to the NCUA systems environment have the same information security measures implemented as NCUA's systems. As a result, NCUA could better ensure that its network is protected against threats and better ensure the confidentiality, integrity, and availability of NCUA data and information systems.

Recommendations: We recommend that NCUA:

8. Designate OCIO as centrally responsible for managing and overseeing the security requirements for NCUA's contractor systems.

Agency Response:

This recommendation requires coordination between multiple offices to recognize OCIO as the party responsible for overseeing security requirements for contractor systems. OCIO will work with relevant offices to update procurement procedures by September 30, 2014.

9. Develop a formal process for maintaining sufficient assurance that security controls for contractor systems are effectively implemented, to include:

[5] SOC 1 reports effectively replaced SAS 70 reports as of June 15, 2011. The reports provide a means of reporting on the system of internal control for purposes of complying with internal control over financial reporting.

a. A centrally maintained and monitored inventory of contractor systems;

b. Periodic review of the system inventory (at least annually) to determine that all systems have been appropriately categorized as agency or contractor systems as well as cloud or non-cloud systems;

c. A centrally maintained and monitored inventory of system interconnections for all NCUA systems that is regularly reviewed (at least annually) for accuracy and that is supported by valid and signed ISAs or MOUs; and

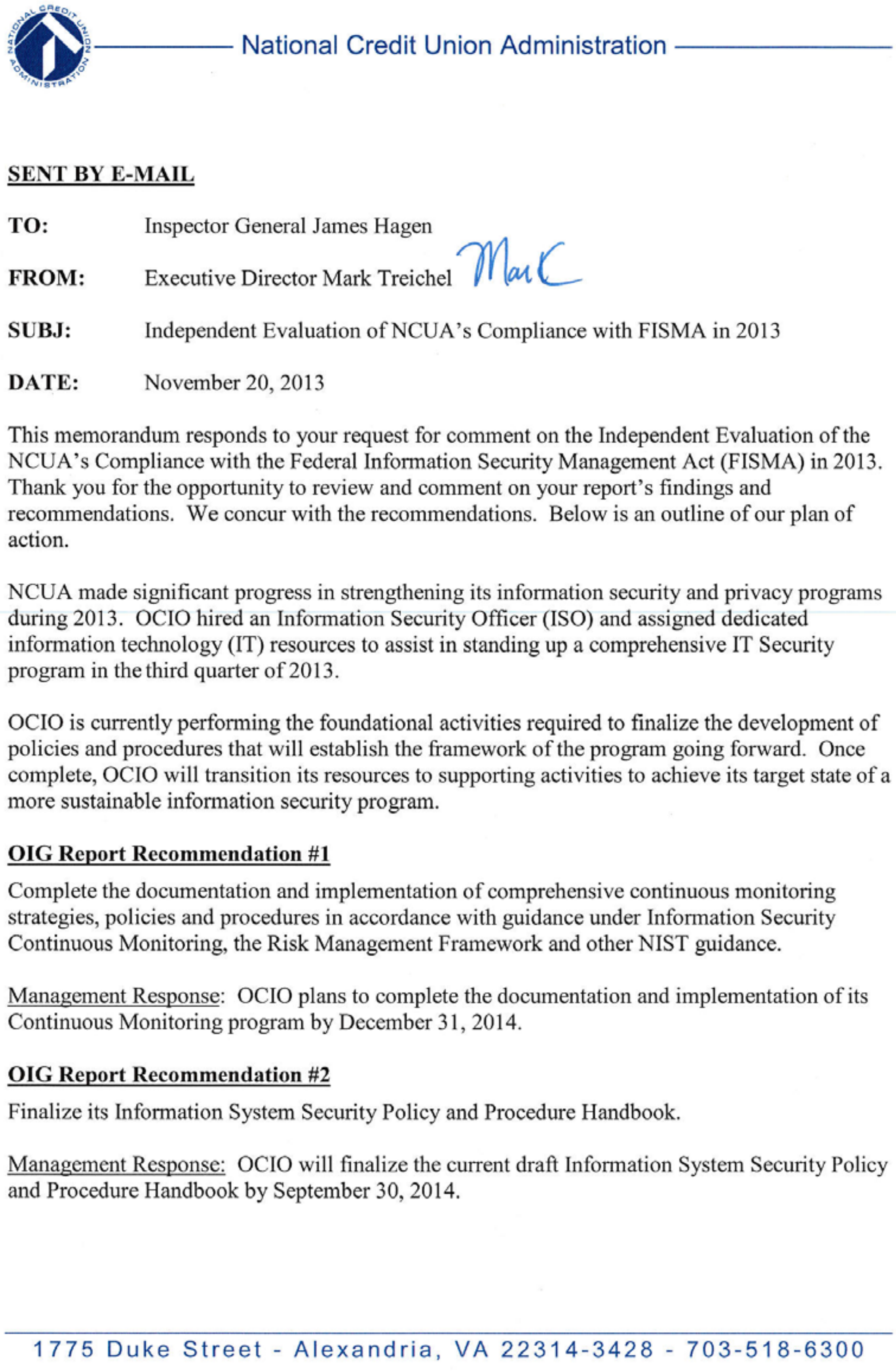
d. A central repository of applicable valid, approved, and signed security documentation (e.g., System Security Plans, Interconnection Security Agreements, etc.) for each of the contractor systems.

Agency Response:

OCIO will update its process for Contractor Systems to address items discussed in the recommendation by September 30, 2014.

OIG Response: The OIG Concurs with management's comments.

Appendix A: NCUA Management Comments



National Credit Union Administration

SENT BY E-MAIL

TO: Inspector General James Hagen

FROM: Executive Director Mark Treichel

SUBJ: Independent Evaluation of NCUA's Compliance with FISMA in 2013

DATE: November 20, 2013

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) in 2013. Thank you for the opportunity to review and comment on your report's findings and recommendations. We concur with the recommendations. Below is an outline of our plan of action.

NCUA made significant progress in strengthening its information security and privacy programs during 2013. OCIO hired an Information Security Officer (ISO) and assigned dedicated information technology (IT) resources to assist in standing up a comprehensive IT Security program in the third quarter of 2013.

OCIO is currently performing the foundational activities required to finalize the development of policies and procedures that will establish the framework of the program going forward. Once complete, OCIO will transition its resources to supporting activities to achieve its target state of a more sustainable information security program.

OIG Report Recommendation #1

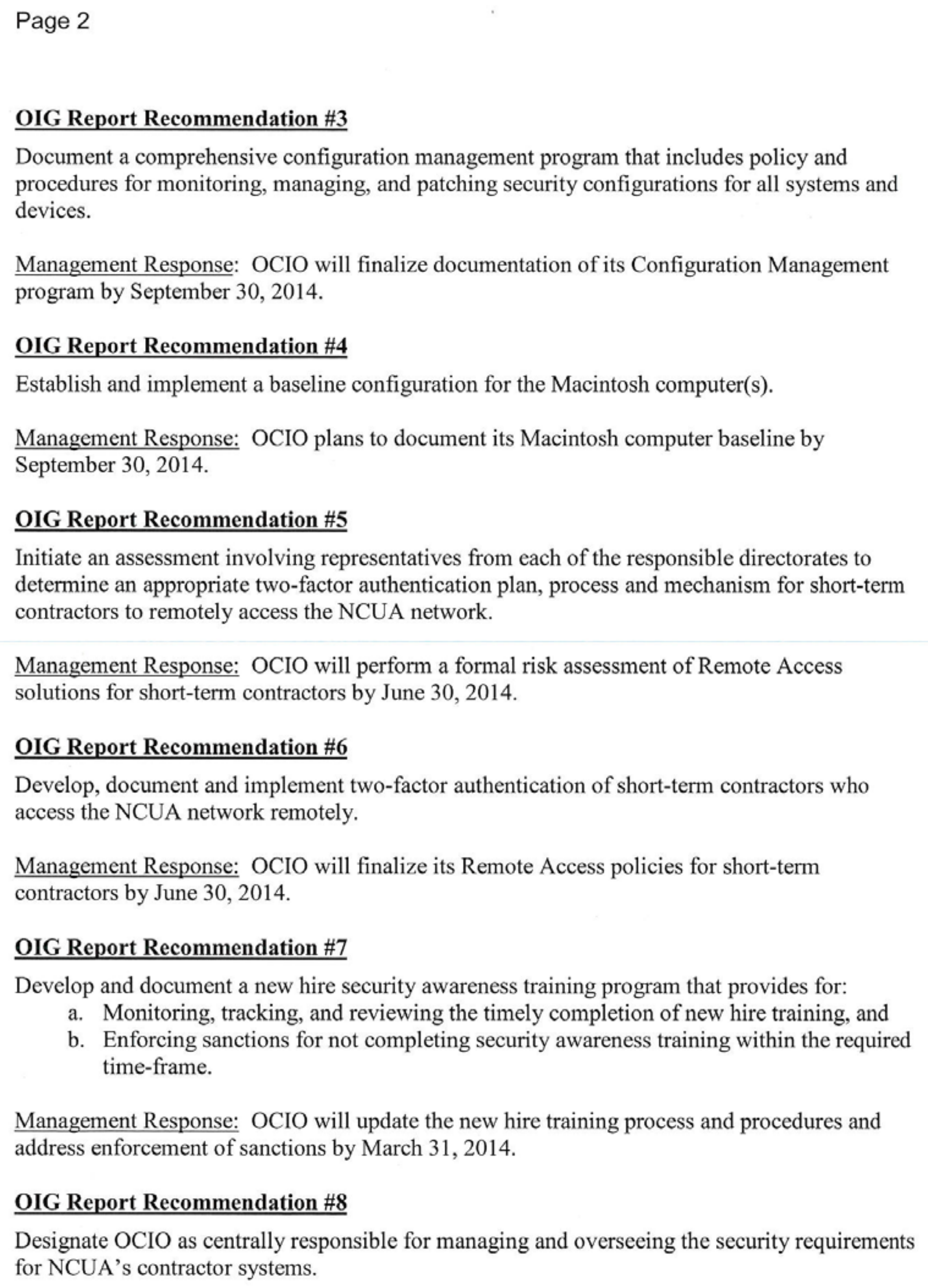
Complete the documentation and implementation of comprehensive continuous monitoring strategies, policies and procedures in accordance with guidance under Information Security Continuous Monitoring, the Risk Management Framework and other NIST guidance.

Management Response: OCIO plans to complete the documentation and implementation of its Continuous Monitoring program by December 31, 2014.

OIG Report Recommendation #2

Finalize its Information System Security Policy and Procedure Handbook.

Management Response: OCIO will finalize the current draft Information System Security Policy and Procedure Handbook by September 30, 2014.



Page 2

OIG Report Recommendation #3

Document a comprehensive configuration management program that includes policy and procedures for monitoring, managing, and patching security configurations for all systems and devices.

Management Response: OCIO will finalize documentation of its Configuration Management program by September 30, 2014.

OIG Report Recommendation #4

Establish and implement a baseline configuration for the Macintosh computer(s).

Management Response: OCIO plans to document its Macintosh computer baseline by September 30, 2014.

OIG Report Recommendation #5

Initiate an assessment involving representatives from each of the responsible directorates to determine an appropriate two-factor authentication plan, process and mechanism for short-term contractors to remotely access the NCUA network.

Management Response: OCIO will perform a formal risk assessment of Remote Access solutions for short-term contractors by June 30, 2014.

OIG Report Recommendation #6

Develop, document and implement two-factor authentication of short-term contractors who access the NCUA network remotely.

Management Response: OCIO will finalize its Remote Access policies for short-term contractors by June 30, 2014.

OIG Report Recommendation #7

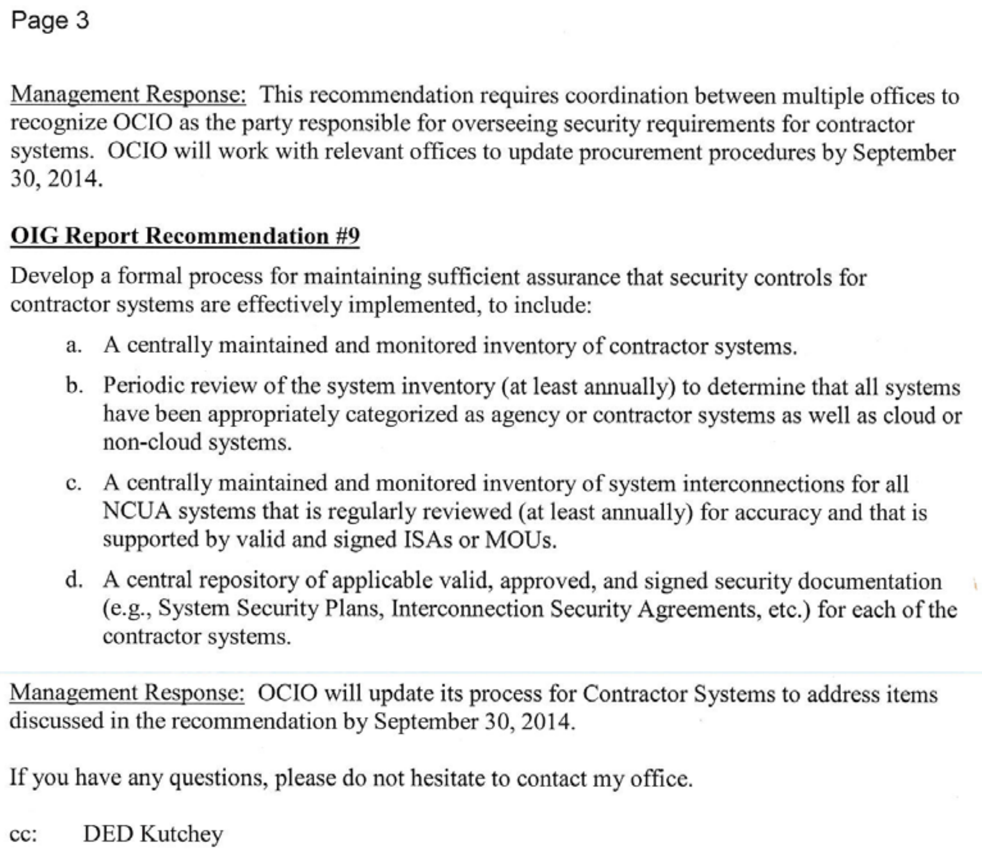
Develop and document a new hire security awareness training program that provides for:

a. Monitoring, tracking, and reviewing the timely completion of new hire training, and
b. Enforcing sanctions for not completing security awareness training within the required time-frame.

Management Response: OCIO will update the new hire training process and procedures and address enforcement of sanctions by March 31, 2014.

OIG Report Recommendation #8

Designate OCIO as centrally responsible for managing and overseeing the security requirements for NCUA's contractor systems.



Page 3

Management Response: This recommendation requires coordination between multiple offices to recognize OCIO as the party responsible for overseeing security requirements for contractor systems. OCIO will work with relevant offices to update procurement procedures by September 30, 2014.

OIG Report Recommendation #9

Develop a formal process for maintaining sufficient assurance that security controls for contractor systems are effectively implemented, to include:

a. A centrally maintained and monitored inventory of contractor systems.

b. Periodic review of the system inventory (at least annually) to determine that all systems have been appropriately categorized as agency or contractor systems as well as cloud or non-cloud systems.

c. A centrally maintained and monitored inventory of system interconnections for all NCUA systems that is regularly reviewed (at least annually) for accuracy and that is supported by valid and signed ISAs or MOUs.

d. A central repository of applicable valid, approved, and signed security documentation (e.g., System Security Plans, Interconnection Security Agreements, etc.) for each of the contractor systems.

Management Response: OCIO will update its process for Contractor Systems to address items discussed in the recommendation by September 30, 2014.

If you have any questions, please do not hesitate to contact my office.

cc: DED Kutchey