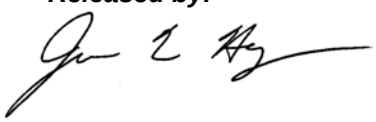
NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 2011

Report # OIG-11-12
November 10, 2011

William A. DeSarno
Inspector General

Released by:



James Hagen
Deputy Inspector General

Auditor-in-Charge:

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 Richard S. Carson and Associates, Inc. (Carson Associates), 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.

Carson Associates evaluated NCUA's security program through interviews, documentation reviews, technical configuration reviews, and sample testing. Carson Associates 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 further strengthen its information security and privacy programs during Fiscal Year (FY) 2011. NCUA's accomplishments during this period include:

- Improved its security configuration for servers and desktops;
- Improved its ability to establish a fully integrated continuous monitoring program by implementing automated software, which includes intrusion detection, vulnerability scanning, and logging tools;
- Developed and implemented policies and procedures for overseeing external service providers;
- Improved its contingency planning program for its FISMA systems;
- Established, implemented and enforced security baselines for its servers and desktop devices;
- Improved its Plan of Action and Milestone process;
- Provided Business Impact Assessments (BIAs) for its FISMA systems and is currently extending the BIA study down to its regional/field offices;
- Improved its procedures for ensuring terminated users and inactive user accounts are disabled or removed from NCUA systems; and
- Implemented continuing education requirements for its information technology employees.

We identified two areas remaining from last year's FISMA evaluation that NCUA officials need to address. NCUA needs to:

- Improve remote access controls; and
- Improve its privacy program (i.e., review its use of Personally Identifiable Information and Social Security Numbers).

In addition, we identified four new findings this year where NCUA could improve its information technology security controls. Specifically, NCUA needs to:

- Improve its continuous monitoring program;

- Improve its security authorization packages;
- Improve its contingency planning program; and
- Improve its intrusion detection policies and procedures.

We appreciate the courtesies and cooperation provided to our staff and Carson and Associates 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 (FISMA)

The President signed into law the E-Government Act (Public Law 107-347), which includes Title III, Information Security, on December 17, 2002. 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 released the FY 2011 reporting metrics (June 1, 2011), 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. OMB issued the FY 2011 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management on September 14, 2011. This document provides instructions to agencies for meeting its reporting requirements under FISMA. In addition, it includes instructions for reporting on agencies' privacy management programs. Furthermore, it includes clarifications to help agencies implement and meet FISMA and privacy requirements.

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 chairman is 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. In addition to its central office in Alexandria, NCUA has five regional offices and the Asset Management and Assistance Center (AMAC).

III. OBJECTIVE

The audit objective was to assist the OIG in performing 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;
- Remediating prior audit weaknesses pertaining to FISMA and other security and privacy weaknesses identified; and
- Implementing its Plan of Action and Milestones (POA&M)

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 the OIG to report to OMB.

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 2011 Inspector General FISMA Reporting Metrics. These areas included: risk management, configuration management, incident response and reporting, security training, POA&M,

remote access management, identity and access management, continuous monitoring management, contingency planning, contractor systems, and security capital planning.

We conducted our fieldwork from August 2011 through November 2011. 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-related and privacy-related controls. NCUA has made progress in addressing last year's reported deficiencies; however, some prior year deficiencies remain. In addition, we identified other areas for improvement that require management's attention. We discuss these issues below.

1. NCUA needs to improve its remote access controls

NCUA only requires one-factor authentication for remote access to its network.

This issue is a repeat finding from the FY 2010 FISMA evaluation.

OMB M-07-16 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.

NCUA has issued PIV cards and uses the cards for physical access to its facilities. However, NCUA officials indicated NCUA has not required the use of the PIV cards for remote authentication to its network because most users forgot their PIN. The majority of NCUA users is not centrally located and works from the field. Therefore, NCUA officials indicated the agency will use its next central agency-wide meeting in April 2012 to issue users new PINs.

By implementing OMB remote access security requirement, NCUA will help protect its systems and data from the risk of unauthorized exposure. Should a breach of information occur (e.g., Financial Sector Oversight information), NCUA's reputation could be hurt and it could have a serious adverse effect on organizational operations, assets, or individuals.

Recommendation 1: We recommend that NCUA management require and implement multifactor authentication for remote access to its network.

Agency Response: *We have delayed resolution of this finding due to logistical and financial concerns and have accepted this risk. We will implement two factor authentication at the national conference. This plan has been communicated to OMB under the requirements of HSPD-12 and PIV implementation.*

OIG Response: The OIG concurs.[1]

[1] NCUA's conference is scheduled for April 2012.

2. NCUA needs to improve its continuous monitoring program.

While NCUA has some automated tools (e.g., intrusion detection, Secure Content Automation Protocol), and policies and procedures that would be components of a continuous monitoring program, NCUA has not completely implemented its continuous monitoring strategy and program. Specifically, the agency does not have documented continuous monitoring policies and procedures and has not fully integrated the various components of its information security program into a strategy that facilitates near real-time monitoring and risk management.

NIST SP-800-37, Revision 1 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.

In addition, continuous monitoring of security controls using automated support tools facilitates near real-time risk management and represents a significant change in the way security authorization activities have been employed in the past. Near real-time risk management of information systems can be facilitated by employing automated support tools to execute various steps in the Risk Management Framework[2] including authorization-related activities. In addition to vulnerability scanning tools, system and network monitoring tools, and other automated support tools that can help to determine the security state of an information system, organizations can employ automated security management and reporting tools to update key documents in the authorization package including the security plan, security assessment report, and plan of action and milestones.

Furthermore, an effective organization-wide continuous monitoring program includes:

- Configuration management and control processes for organizational information systems;

- Security impact analyses on proposed or actual changes to organizational information systems and environments of operation;

[2] The Risk Management Framework is a six-step process, which essentially replaces the traditional Certification and Accreditation process. The intent of this common framework is to improve information security, strengthen risk management processes, and encourage reciprocity among federal agencies.

- Assessment of selected security controls (including system-specific, hybrid, and common controls) based on the organization-defined continuous monitoring strategy;

- Security status reporting to appropriate organizational officials; and

- Active involvement by authorizing officials in the ongoing management of information system-related security risks.

By formally establishing a continuous monitoring strategy and program, NCUA can meet Federal requirements for continuous near real-time monitoring of its information security program, which would enhance its ability to maintain the confidentiality, integrity, and availability of NCUA systems and data.

Recommendation 2: We recommend that NCUA management document and implement its continuous monitoring strategies, policies and procedures under the Risk Management Framework.

Agency Response: *OCIO will develop over-arching policy that establishes the parameters of agency continuous monitoring. This policy will include a newly established security calendar with all security events to ensure continuous monitoring of all recurring events. OCIO will also update policy to articulate what items must be included in the calendar. Existing monitoring of the IDS will not be included in the calendar as that is a real-time system.*

OIG Response: The OIG concurs.

3. NCUA needs to improve its security authorizations.

NCUA's Asset Management and Assistance Center (AMAC) security plan does not address each of the minimum security controls applicable to the system's security categorization. In addition, the AMAC security plan does not match the control families identified in SP 800-53. For example, the AMAC security plan does not address the security controls for Risk Assessment Policy and Procedures, Security Categorization, Risk Assessment, and Vulnerability Scanning as required by SP 800-53.

NIST SP 800-53, Revision 3 provides guidelines for selecting and specifying security controls for information systems supporting the executive agencies of the Federal government to meet the requirements of FIPS 200. The guidelines apply to all components of an information system that process, store, or transmit Federal information. The guidelines have been developed to help achieve more secure information systems and effective risk management within the Federal government by:

- Facilitating a more consistent, comparable, and repeatable approach for selecting and specifying security controls for information systems and organizations; and

- Providing a recommendation for minimum security controls for information systems categorized in accordance with FIPS 199, Standards for Security Categorization of Federal Information and Information Systems.

NCUA officials indicated the AMAC security plan is outdated because it was prepared under NIST SP 800-26 (April 2005). NIST superseded this guidance with NIST SP 800-53. The current guidance is NIST SP 800-53, Revision 3, dated August 2009.

By having security authorization packages that meet current government standards, NCUA can help eliminate or reduce potential system vulnerabilities. Ultimately, this could help protect the confidentiality, integrity, and availability of NCUA's systems and data.

Recommendation 3: We recommend that NCUA management update the AMAC security plan to comply with current Federal standards and guidance.

Agency Response: *OCIO will work with AMAC to update the AMAC security plan and include it as another appendix to the GSS security plan. This will consolidate all NCUA systems into one system and more closely align our operations with the new continuous monitoring model set forth by OMB.*

OIG Response: The OIG concurs.

4. NCUA needs to improve its contingency planning program.

NCUA's contingency plan for its AMAC system is three years old and outdated. In addition, NCUA has not tested the contingency plan within the past year.

OMB Circular A-130 requires agencies to establish and periodically test the capability to perform the agency function supported by the application in the event of failure of its automated support.

NIST SP 800-34, Revision 1 requires agencies to ensure contingency plan maintenance. The guidance indicates the plan should be a living document that is updated regularly to remain current with system enhancements and organizational changes.

NCUA officials informed us the agency has not updated and tested the AMAC contingency plan because the system is undergoing a modification where major portions of the system will reside on the NCUA General Support System.

Updating and testing the AMAC system contingency plan will reduce the potential impact on AMAC in the event its system becomes nonoperational. NCUA can minimize its efforts to recover AMAC with an accurate, current and tested contingency plan.

Recommendation 4: We recommend that NCUA management update and test the AMAC system contingency plan.

Agency Response: *OCIO will work with AMAC to complete the existing effort to add part of the AMAC operation to the GSS contingency plan and have that data available at the DR site. OCIO will assist AMAC to update the existing contingency plan to address all other residual data and the AFTECH system.*

OIG Response: The OIG concurs.

5. NCUA needs to improve its intrusion detection policies and procedures.

In response to the OIG's FY 2010 independent evaluation of NCUA's compliance with FISMA, NCUA indicated it was implementing in-house intrusion detection in place of using a third-party service provider. In addition, NCUA indicated it would implement procedures governing security parameters and response times to adequately secure its perimeter. While NCUA has since implemented in-house intrusion detection, and developed intrusion detection policies and procedures, its policies and procedures do not include response times for addressing vulnerabilities. In addition, NCUA does not have a means to monitor the remediation of vulnerabilities through completion.

NIST SP 800-137 guides that within the context of an information system continuous monitoring program, intrusion detection/prevention systems (IDPSs) can be used to supply evidence of the effectiveness of security controls (e.g., policies, procedures, and other implemented technical controls), document existing threats, and deter unauthorized use of information systems. IDPSs may also provide supporting data to assist organizations in meeting US-CERT incident reporting requirements and in responding to OMB and agency CIO reporting requirements in the areas of system and connections inventory, security incident management, boundary protections, and configuration management.

By documenting specific security considerations, response time requirements and other guidelines in intrusion detection policies and procedures, NCUA management would institutionalize formal guidelines that would help maintain the confidentiality, availability, and integrity of NCUA data and systems.

Recommendation 5: We recommend that NCUA management:

- Update its Intrusion Detection policies and procedures to establish maximum allowable response times for addressing security incidents.

- Implement a tracking system to monitor the status of vulnerabilities.

Agency Response: *OCIO has updated the GSS with timelines and will document specific procedures to track vulnerabilities to resolution.*

OIG Response: The OIG concurs.

6. NCUA needs to improve its privacy program.

While NCUA staff indicated the agency has performed a limited inventory of Personally Identifiable Information (PII), NCUA has not performed a complete review of its holdings of PII, and if necessary, reduced its use of PII and Social Security Numbers (SSNs).

This is a repeat finding from the FY 2010 FISMA Review.

NIST SP 800-122 guides that:

- Organizations should identify all PII residing in their environment.

- Organizations should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission. The likelihood of harm caused by a breach involving PII is greatly reduced if an organization minimizes the amount of PII it uses, collects, and stores.

OMB M-07-16 required that:

- Agencies review current holdings and reduce the volume of PII.

- Reduce the use of Social Security Numbers and eliminate any unnecessary use, and explore alternatives for a personal identifier for both Federal employees and in Federal programs.

- Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual reports under FISMA. Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act Systems of Records Notices (SORN).

- Within 120 days from the date of the memo (May 22, 2007), agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of Social Security Numbers within eighteen months.

By performing a review to determine the amount of PII and use of SSNs at NCUA, and if necessary, reducing the amount of PII and use of SSNs, NCUA will reduce the risk of exposing its sensitive data to a breach of confidentiality by an authorized or unauthorized entity. Ultimately, this could prevent public embarrassment for the agency and a loss of trust by the public.

Recommendation 6: We recommend that NCUA management:

- Review current holdings of Personally Identifiable Information and, if necessary, develop a plan to reduce any unnecessary use of PII and provide progress updates.

- Review and if necessary, create and execute a schedule to eliminate any unnecessary collection and use of Social Security Numbers, and if applicable, explore alternatives for a personal identifier for Federal employees and in Federal programs.

Agency Response: *The Office of General Counsel agrees with the recommendations. In September 2011, our Office was reorganized with a section devoted to Administrative Law. This section is now responsible for issues arising out of the Privacy Act and the Associate General Counsel for Administrative Law is now the Senior Agency Official for Privacy. Privacy issues, including identification and elimination of unnecessary SSNs and other PII, will be given a higher priority. Working with the Office of Human Resources, the Office has begun privacy training for supervisory personnel. In the 2012 fiscal year, the Office will develop an inventory of PII and plans to work with the Office of Chief Information Officer in implementing software they have obtained to identify SSNs and to then reduce any unnecessary use of PII, including SSNs.*

OIG Response: The OIG concurs.