NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION INFORMATION SECURITY PROGRAM 2007

Report #OIG-07-09 **September 12, 2007**

William A. DeSarno
Inspector General

Released by:

James Hagen
Asst IG for Audits

Auditor-in-Charge:

W. Marvin Stith, CISA
Sr Information Technology Auditor

INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION
INFORMATION SECURITY PROGRAM - 2007
Report #OIG-07-09

CONTENTS

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged Grant Thornton LLP to independently evaluate its 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.

Grant Thornton evaluated NCUA's security program through interviews, documentation reviews, technical configuration reviews, social engineering testing, and sample testing. We evaluated NCUA against standards and requirements for federal government agencies such as those provided through FISMA, National Institute of Standards and Technology (NIST) Special Publications (SPs), and Office of Management and Budget (OMB) memorandums. We conducted an exit conference with NCUA on June 29, 2007, to discuss evaluation results.

The NCUA made noticeable progress in strengthening its Information Technology (IT) security program during Fiscal Year (FY) 2007. Notable accomplishments include:

- Completion of Certification and Accreditation packages for all of its FISMA systems.
- Implementation of additional encryption protection for data on examiner laptops.

While NCUA made commendable progress in addressing the deficiencies reported last year, management could still improve IT security controls in the following areas:

- NCUA needs a better document management program.
- NCUA has not implemented continuing education requirements for its Information Technology employees.
- Employee enter/exit/change procedures do not ensure timely removal of terminated employees' access to NCUA systems.
- E-Authentication risk assessments for its systems need to be completed.
- A formal agency-wide security configuration guide should be developed.
- Incident response procedures should be followed.
- Personnel security awareness training needs to be completed in FY 2007.
- NCUA's Plan of Actions and Milestones (POA&M) process needs improvement.
- Security controls testing for all of NCUA's FISMA systems needs to be completed.
- Segregation of duties should be maintained or compensating controls established.
- NCUA vulnerability management needs improvement.

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

.

II. BACKGROUND

This section provides background information on FISMA and 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. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues 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.

OMB issued the 2007 Reporting Instructions for the Federal Information Security Management Act on July 25, 2007. This document provides clarification to agencies for implementing, meeting, and reporting FISMA requirements to OMB and Congress.

NATIONAL CREDIT UNION ADMINISTRATION (NCUA)

NCUA is the independent federal agency that charters, supervises, and insures the nation's federal credit unions, and it 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 appointed by the President of the United States and confirmed by the Senate. The Board consists of a chairman, vice chairman, and member. No more than 2 board members can be from the same political party, and each member serves a

staggered 6-year term. NCUA's 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 engagement objective was to assist the OIG in performing an independent evaluation of NCUA information security 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 program
- Meeting responsibilities under FISMA
- Remediating prior audit weaknesses relating to FISMA and other security weaknesses identified
- Implementing its plans of action and milestones (POA&M)

Additionally, the audit was required to provide sufficient supporting evidence of NCUA's security program evaluation to enable the OIG to report to OMB.

IV. METHODOLOGY AND SCOPE

We compared NCUA's information security program and practices with FISMA and federal criteria contained in the Government Accountability Office's *Federal Information System Controls Audit Manual (FISCAM)*, as well as other relevant guidance from NIST and OMB.

We reviewed information security control techniques for all of NCUA's major information systems on a rotational basis. During this evaluation, we assessed NCUA controls over security planning and program management, segregation of duties, security awareness training, and performed a limited scope vulnerability assessment. In addition, we evaluated additional areas required to report under OMB M-07-19 such as reviews of Certification and Accreditation (C&A) documentation including system security plans, risk assessments, contingency plans, and certification reports. Furthermore, we reviewed existing information security controls and identified weaknesses impacting certain components affecting General Support System (GSS) security.

We conducted a focused vulnerability assessment this year over NCUA's SAP system, Voice Over Internet Protocol (VOIP), and the Automated Integrated Regulatory Examination System (AIRES).

We performed our engagement in accordance with generally accepted government auditing standards (GAGAS), audit standards promulgated by the American Institute of Certified Public Accountants (AICPA), and information systems standards issued by the Information Systems Audit & Control Association (ISACA).

V. RESULTS IN DETAIL

Security program planning and management controls are designed to provide the framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an entity's computer-related controls. While NCUA made commendable progress in addressing the deficiencies reported last year, management could still improve IT security controls as discussed below.

1. NCUA needs a better document management program.

NCUA's has improved its document management since FY 06. However, management has still not established an effective document management program. We inspected security policies, plans and procedures, but could not readily identify the most current version of some of the documents. In addition, officials did not always periodically update documents (e.g., individual system security plans did not include current GSS security categorizations). Furthermore, management was not required to approve revisions/updates of security documentation.

By not establishing a document management system to facilitate the NCUA Information Technology (IT) security program, NCUA may not be adequately protecting itself from security threats in a continually changing and risk inherent IT environment.

The NIST Special Publication 800-53 *Recommended Security Controls for Federal Information Systems* provides guidance related to these conditions:

> *Agencies should plan, develop, and disseminate all plans, policies and procedures to facilitate security planning and planning controls; obtain appropriate review and approval for the security plan; and address system/organizational changes or problems identified during plan implementation or security control assessments.*

Recommendation: We recommend that NCUA improve its document management process, including version controls, timely documentation updates and management approvals.

Agency Response: Agreed.

OIG Response: The OIG concurs.

2. NCUA has not implemented continuing education requirements for its Information Technology employees.

While all NCUA employees are required to participate in annual security awareness training, NCUA does not require IT employees to obtain additional security related training. Additionally, we determined that NCUA employee training records and related documentation are not centrally managed and are not readily available. For example:

- NCUA does not track external training taken by employees. Many employees do not submit training requests on the Standard Form -182 and may submit their requests via memo or e-mail.

- Although the Office of Human Resources is supposed to approve all training requests, it is possible that the employees selected for testing took training and NCUA has not recorded it.

The NCUA Training Guide encourages employees to request training needs, but there are no expected continuing education requirements for IT employees. The guide does not define the number of training hours an employee should receive nor does it provide for a means of tracking training received. This tracking may be in the form of education units, CPE, etc.

By not requiring IT employees to take security related training and not defining a training requirement program, IT employees may not have the most current technical knowledge to effectively protect the confidentiality, integrity, and availability of its systems and sensitive data.

The NCUA Agency Wide Information Security Policy provides guidance related to this condition:

> *Section 3.1.3 requires: "Training oversight has two parts, general awareness training and specific training for people with significant security responsibilities. The CIO will review the reports specified in section 3.2.3 to ensure adequate training is planned for NCUA."*

OMB Memorandum 06-20 also provides guidance related to this condition:

> *Section C, Item 9 inquires if the agency has ensured that security training and awareness has been provided to all employees, including contractors and those employees with significant IT security responsibilities.*

NIST SP 800-53 also provides guidance related to this condition:

> *Section AT-3 states that the organization ensures system managers, system administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties.*
>
> *Section AT-4 states that the* organization documents and monitors individual information system security training activities including basic security awareness training and specific information system security training.

Recommendation: We recommend that NCUA set forth expected continuing education requirements within the NCUA Training Guide for its IT employees and implement a mechanism to effectively track and report training taken.

Agency Response: Agreed.

OIG Response: The OIG concurs.

3. Employee enter/exit/change procedures do not ensure timely removal of terminated employees' access to NCUA systems.

Although NCUA has documented employee enter/exit/change procedures, they are outdated and do not accurately define responsibilities. NCUA management has not updated the procedures since 1998. In addition, request for removal of a user account does not always occur timely. Furthermore, we determined that seven terminated employees still had user accounts which would allow them access to the NCUA network.

By not having updated, documented employee enter/exit/change procedures, NCUA employees who have a role in the termination process may not fully understand their roles and responsibilities. In addition, by not removing terminated employees' access to systems and or applications, NCUA increases the risk that unauthorized persons could access NCUA systems and sensitive data.

The NCUA Computer Infrastructure System Security Plan provides guidance related to these conditions:

> *The NCUA Computing Infrastructure System Security Plan requires that the procedures found in its appendix for adding, changing and deleting an NCUA employee from the network be used.*
>
> *This procedure guides that when an employees enters, exits or needs changes to their employee information, the responsible office will e-mail information (where applicable) to the appropriate distribution lists.*

NIST SP 800-12, *An Introduction to Computer Security: The NIST Handbook,* also provides guidance related to these conditions:

> *Section 10.2.1 User Account Management, states when user accounts are no longer required, the supervisor should inform the application manager and system management office so accounts can be removed in a timely manner.*

Recommendation: We recommend that NCUA update their Windows Active Directory list to remove all employees that are no longer with the agency. In addition, NCUA should update their employee enter/exit/change procedures in an effort to provide management with a means of enforcing responsibility and accountability for all employees involved in the termination process.

Agency Response: Agreed. We have since updated the Windows Active Directory and have a mechanism in place to keep it current. NCUA will look for ways to improve the employee enter/exit/change.

OIG Response: The OIG concurs with the actions taken

4. E-Authentication risk assessments for its systems need to be completed.

While NCUA has completed formal risk assessments for its six (6) systems, NCUA did not specifically address E-Authentication risk considerations. This finding is a repeat finding from

the FY 06 FISMA evaluation. NCUA has asserted that the requirement to complete an E-Authentication risk assessment does not apply to the agency and therefore NCUA has not completed the assessment.

By not completing an E-Authentication risk assessment, the NCUA is not compliant with OMB policy and may not fully capture risks associated with their e-Government activities.

OMB Memorandum M04-04 provides guidance related to this condition:

> *Section 1.1, states that this guidance requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. Additionally, section 1.2 states that it applies to the remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government).*

Recommendation: We recommend that NCUA management complete the E-Authentication risk assessment process in accordance with OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.

Agency Response: Agreed.

OIG Response: The OIG concurs.

5. A formal agency-wide security configuration guide should be developed.

Although the NCUA requires workstations (Windows 2000) and servers (Windows 2003) to have baseline configurations that follow NIST configuration guidance, the NCUA has not developed a formal agency-wide security configuration guide. This is a repeat finding from the FY 06 FISMA evaluation.

By not establishing and implementing a formal security configuration guide, the NCUA increases the risk of not consistently applying security standards across agency information technology resources. This could expose the NCUA systems and sensitive data to threats in the ever changing and risk inherent IT environment.

OMB Memorandum 06-20 provides guidance related to this condition:

> *Section C, Item 6 inquires if there is an agency wide security configuration policy and whether configuration guides are implemented for agency systems running certain software.*

Recommendation: We recommend that NCUA management establish and implement an agency-wide security configuration guide.

Agency Response: Agreed. The security plan has been updated to require NIST configuration standards for all servers. We will run the base-line analyzer to ensure these standards are met.

OIG Response: The OIG concurs.

6. Incident response procedures should be followed.

NCUA has an established incident response capability that is documented in an Incident Response Guide. However, evidence could not be provided for the one incident identified by management during FY 06 to support whether NCUA followed their incident response steps outlined in their guide. These steps include processes for identifying and reporting incidents internally, for external reporting to law enforcement authorities, and for reporting to the United States Computer Emergency Readiness Team (US-CERT).[1]

By not documenting how NCUA addresses incidents, NCUA is not compliant with OMB policy. In addition, management is not able to determine whether NCUA followed its incident response procedures outlined in the Incident Response Guide and whether employees understand the incident response procedures. This issue may also prevent NCUA from responding in a systematic manner to incidents and carrying out all necessary steps to correctly handle an incident in the future. Adequately documenting incidents could prevent or minimize disruption of critical computing services and minimize loss or theft of sensitive or mission critical information.

NCUA's Incident Response Guide provides guidance related to this condition:

> *Section 4.6 "Follow up" requires NCUA to document its response to an incident and use "lessons learned" to update computer security measures.*

OMB Memorandum 06-20 also provides guidance related to this condition:

> *Section C, Item 7 inquires if the agency follows documented policies and procedures for identifying and reporting incidents internally, for external reporting to law enforcement authorities, and for reporting to the United States Computer Emergency Readiness Team (US-CERT).*

Recommendation: We recommend that NCUA management comply with the requirements of OMB Memorandum 06-20, Section C, Item 7, and specifically, with its incident response procedures contained within the Incident Response Guide.

Agency Response: Agreed. We will document all further incidents in compliance with our incident response guide and OMB guidance.

OIG Response: The OIG concurs.

7. Personnel security awareness training program needs to be completed in FY 2007.

The NCUA has established an information security awareness program. However, as of the time of our assessment, NCUA employees had not received annual security awareness training

[1]The Information Security Officer stated that no incidents occurred during FY 07. One incident occurred during FY 06 and it was being investigated at the time Grant Thornton performed the FY 06 FISMA review. Since we were unable to inspect the incident in FY 06, we requested information/documentation on the FY 06 incident as part of this year's audit.

for FY 07. This is a repeat finding from the FY 06 FISMA evaluation. NCUA employees have not received annual security awareness training for FY 07 because NCUA is revising the NCUA Rules of Behavior document to include a section on privacy issues. NCUA will continue its training efforts once this process is completed.

By not having all employees' complete security awareness training, NCUA is not compliant with OMB policy. In addition, untrained employees may expose NCUA to threats, which put confidentiality, integrity, and availability of NCUA systems and sensitive data at risk.

The NIST SP 800-50, *Building an Information Technology Security Awareness and Training Program* provides guidance related to these conditions:

> *Agencies must establish an effective security awareness and training program to ensure that users are appropriately trained in the rules of behavior for the systems and applications to which they have access. In addition, the guidance tasks the Chief Information Officer with ensuring that effective tracking and reporting mechanisms are in place.*

OMB Memorandum 06-20 also provides guidance related to this condition:

> *Section C, Item 9 inquires if the agency has ensured that security training and awareness has been provided to all employees, including contractors and those employees with significant IT security responsibilities.*

Recommendation: We recommend that NCUA management comply with the requirements of OMB Memorandum 06-20, Section C, Item 9, by ensuring that all employees and contractors receive annual security awareness training by signing the NCUA Rules of Behavior document.

Agency Response: Agreed.

OIG Response: The OIG concurs.

8. NCUA's Plan of Actions and Milestones (POA&M) process needs improvement.

NCUA program officials are not actively involved in tracking and updating the Plan of Actions and Milestones (POA&M) for their respective systems. In addition, none of 12 IT-related findings identified in the 2006 financial statement audit report issued by Deloitte & Touche LLP were included in the POA&M. Further, there were three FY 06 FISMA report findings that were considered complete in the POA&M that were not addressed or fully completed by NCUA:

- E-Authentication risk assessments not completed
- Security configuration guides not used for all NCUA systems
- Security planning documentation inconsistent in version control, revisions/updates

We reviewed documentation and interviewed the NCUA Information Security Officer (ISO). We found the POA&M process is largely driven by updates from the ISO, instead of the ISO receiving periodic updates from program officials responsible for remediation requirements.

Program officials are not actively identifying vulnerabilities or weaknesses and incorporating them into existing POA&Ms.

As a result, the NCUA ISO faces the additional burden of tracking agency efforts to reduce risk and vulnerabilities by having to actively pursue status updates from program officials for their respective action items. Weaknesses that program officials identify in the POA&M, but do not properly address and resolve reduce NCUA's level of compliance with OMB requirements.

OMB and FISMA require agency officials to be involved in agency efforts to review and periodically update remediation efforts to correct outstanding weaknesses. In most cases, agencies use a POA&M process to track these efforts, which is intended to be a tool for the program official to note changes and updates, usually on a quarterly basis.

Recommendation: We recommend that NCUA management implement and enforce policy that requires program officials to provide POA&M status reports to the OICO. In addition, the ISO should ensure all identified weaknesses are incorporated into the POA&M.

Agency Response: Agreed.

OIG Response: The OIG concurs.

9. Security controls testing for all of NCUA's FISMA systems needs to be completed.

The NCUA completed security controls testing in FY 07 for its General Support System (GSS) system. However, NCUA has not completed its FY 07 security controls testing for the remainder of its five FISMA systems (AMAC, NAS, ESS, CRS, and IIS). The NCUA anticipates security testing and evaluation efforts for all of NCUA's systems to begin in late June and finish in August.

Until NCUA completes security controls testing for its systems, it may not know whether security controls in place are operating effectively. This may prevent NCUA from appropriately mitigating risks to an acceptable level.

As required in FISMA, the CIO shall evaluate a representative subset of systems, including information systems used or operated by an agency or by a contractor of an agency or other organization on behalf of an agency. OMB requires agencies to have tested security controls within the past year.

Recommendation: We recommend that NCUA management complete security controls testing for its FISMA systems using guidance specified by NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*. NCUA should tailor its security controls testing based on the FIPS 199 rankings assigned to each FISMA system.

Agency Response: Agreed – most are now complete.

OIG Response: The OIG concurs.

10. Segregation of duties should be maintained or compensating controls established.

We determined that NCUA does not maintain effective segregation of duties for personnel. Segregation of duties issues exist in the following:

- MSSQL database maintenance and development,
- web application development, and
- SAP maintenance and development.

We identified 56 segregation of duties violations when we scanned and analyzed the SAP application. Additionally, two individuals interviewed revealed that they not only develop code, but also promote code to the production environment, thereby violating best practices and segregation of duties for application change management. We also found NCUA management has not identified incompatible duties and appropriately divided those duties among personnel.

Management has indicated that although the NCUA recognizes the value of formal segregation of duties, resource constraints prohibit a comprehensive implementation throughout the organization. However, management has not articulated specific residual risk with segregation of duties constraints, nor defined compensating controls as required.

Because NCUA has not implemented comprehensive segregation of duties over its operational systems and among its support personnel, the potential for fraud and error increases throughout various systems and processes. The impact of this condition has the potential to reach the external web presence of the organization, any database-reliant applications, and SAP data and procedures.

NIST Special Publication 800-53 provides guidance related to this condition:

> *Control AC-5 states that information systems should enforce separation of duties through assigned access authorizations. The organization should establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.*

OMB A-130, Appendix III also provides guidance related to this condition:

> *It has long been recognized that the greatest harm has come from authorized individuals engaged in improper activities, whether intentional or accidental. In every general support system, a number of technical, operational, and management controls are used to prevent and detect harm. Such controls include individual accountability, 'least privilege,' and separation of duties.*
>
> *Separation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code, while another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.*

Recommendation: We recommend that NCUA management: (1) examine existing roles and responsibilities to identify incompatible duties - such an effort will also require the refinement of currently ambiguous job descriptions, (2) define residual risk associated with segregation of duties conditions created by organizational constraints, and (3) establish compensating controls and ensure those controls are included in annual testing.

Agency Response: We agree in principle. Due to the size of our office, we will need to review each of these items and determine if there is anything we can improve.

OIG Response: The OIG concurs.

11. NCUA vulnerability management needs improvement.

We determined that a remote version of Remote Desktop Protocol Server (Terminal Service) is running on the SAP server. This vulnerability could allow an attacker to intercept and encrypt communications between a client and server and obtain sensitive information such as passwords. Additionally, we discovered several ports/communication services available on the SAP and AIRES servers may be unnecessary. NCUA does not periodically evaluate the number of open ports and services on their servers in accordance with an established process of managing vulnerabilities and secure configurations.

By not restricting the number of ports and communication services NCUA increases the risk of an unauthorized person gaining access to the systems. Management should correlated ports and services to a business need and the services required to meet that business need.

NIST SP 800-53 provides guidance related to this condition:

> *Appendix F, CA-2 states the organization conducts an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting the security requirements for the system.*

Recommendation: We recommend that NCUA management review the need for the Remote Desktop Protocol Server on the SAP server. If valid, we recommend that NCUA implement steps to address the weakness, such as requiring the use of Secure Socket Layer (SSL) for this service.

We also recommend that NCUA management implement a procedure to periodically review the number of open ports and services on NCUA servers to assess whether there is a business need for them to be active.

Agency Response: Agreed.

OIG Response: The OIG concurs.