NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION INFORMATION SECURITY PROGRAM 2008

Report #OIG-08-08 **September 24, 2008**

William A. DeSarno

William A. DeSarno
Inspector General

Released by:

James Hagen
Asst IG for Audits

Auditor-in-Charge:

W. Marvin Stith, CISA
Sr Information Technology Auditor

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 July 23, 2008, to discuss evaluation results.

The NCUA has worked to further strengthen its information technology (IT) security program during Fiscal Year (FY) 2008. NCUA's accomplishments during this period include:

- Implementing OMB guidance in managing Privacy and breach notifications.
- Ninety-seven percent of NCUA employees completed annual security awareness training.

We identified six areas remaining from last year's FISMA evaluation that still need improvement:

- NCUA has not adequately established segregation of duty controls for its applications.
- NCUA has not completed E-Authentication risk assessments for its systems.
- NCUA has not completed security controls testing for one of its FISMA systems.
- NCUA does not have a formal agency-wide security configuration guide.
- NCUA has not updated its employee enter/exit/change procedures.
- NCUA has not implemented continuing education requirements for its IT employees.

In addition, we identified four new findings this year where NCUA could improve IT security controls:

- NCUA's System Software Change Procedures needs improvement.
- NCUA vulnerability management needs improvement.
- NCUA lacks a comprehensive contingency planning program for its FISMA systems.
- NCUA's Plans of Action and Milestones (POA&M) process 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 2008 Reporting Instructions for the Federal Information Security Management Act on July 16, 2008. 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 of Directors (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 two board members can be from the same political party, and each member serves a staggered six-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 IT 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 IT 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 IT security program evaluation to enable the OIG to report to OMB.

IV. METHODOLOGY AND SCOPE

We compared NCUA's information technology (IT) 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 IT 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-08-21 such as reviews of Privacy and breach notification, Certification and Accreditation (C&A) documentation including system security plans, risk assessments, contingency plans, and certification reports. Furthermore, we reviewed existing IT security controls and identified weaknesses impacting certain components affecting the General Support System (GSS), application security (to include change controls and configuration management) and service continuity.

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. NCUA has made progress addressing last year's reported deficiencies; however, some deficiencies remain. In addition, we identified other areas for improvement that require management's attention as discussed below.

1. NCUA has not adequately established segregation of duty controls for its applications.

NCUA does not have adequate change controls or controls for segregation of duties[1] in place for its applications. Specifically we found that:

- Programmers for FISMA applications (the NCUA Accounting System, the Call Report System, and the Insurance Information System) are improperly authorized access to both development and production application environments.

- A single SAP administrator has sole responsibility for managing system operations in the production SAP R/3 application.

- One senior programmer has access to all of the NCUA production environments without documented justification or compensating controls.

- NCUA has not documented and implemented policy and procedures enforcing periodic supervisory review and monitoring of programmer activities.

- AMAC's security plan addresses procedures for implementing major or substantial changes to software. However, NCUA does not have documented change control procedures for commercial-off-the-shelf (COTS)[2] software in general. In addition, NCUA could not provide evidence to support that management approved the implementation of changes to the AMAC AFTECH COTS application after they were tested.

This is a repeat finding from the FY 2007 FISMA evaluation.

The OCIO has indicated that although NCUA recognizes the value of formal segregation of duties on application change management, resource constraints prohibit a comprehensive implementation throughout the organization. However, by not

[1] Segregation 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.

[2] COTS is software or hardware that is ready-made and available for sale, lease, or license to the general public. It is often used as an alternative to in-house developments.

restricting programmer access to production environments, NCUA increases the risk that intentional or unintentional error, alteration, or deletion of data within the FISMA systems may occur. This could negatively impact NCUA by affecting the quality and accuracy of the data it provides to its customers and its examiners.

NIST Special Publication 800-53 indicates that information systems should enforce segregation 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.

In addition, FISCAM CC-2 indicates a disciplined process for testing and approving new and modified programs prior to their implementation is essential to make sure programs operate as intended and that no unauthorized changes are introduced.

Recommendation 1: We recommend that OCIO:

1) Examine existing roles and responsibilities of all OCIO programmers/computer specialists/SAP administrators and define residual risks associated with segregation of duties conditions created by organizational constraints.

2) Establish and implement compensating controls if segregation of duties conflicts cannot be easily resolved.

3) Document COTS change control procedures in the NCUA Software Development Handbook.

Agency Response: Agree. We would like to clarify two items:

- The SAP administrator is not responsible for any application development and therefore, segregation of duties does not seem to apply here.
- Each security plan covers COTS change control procedures. We will update the AMAC security plan to make sure there is adequate documentation authorizing updates to the AFTECH system.

OCIO will:

1) Do a complete review of the existing roles and responsibilities of all programmers, computer specialists and SAP administrators and define the segregation of duties risks within our organization.
2) Implement compensating controls for any remaining segregation of duties conflicts.
3) Document change control procedures in the NCUA Software Development Handbook.

OIG Response: The OIG concurs with the planned corrective actions. The OIG notes that controls for segregation of duties are not limited to application development responsibilities. Any position that performs a task within a manual or automated system is subject to segregation of duties. Therefore, segregation of duties would apply to the SAP administrator. However, the OIG also notes management indicated it would include a review of SAP administrators in its review of segregation of duties roles and responsibilities.

2. NCUA needs to improve its System Software Change Procedures.

NCUA has documented change requests and executions for various system software components. However, change control records are neither comprehensive nor sufficiently detailed. In addition, the NCUA Information Security Officer (ISO) maintains the records for change requests in an email archive. However, the ISO does not maintain corresponding records of approval and change execution. Furthermore, some of the NCUA change requests do not adequately document the change. Specifically, we sampled 22 changes and determined:

- Four changes are missing two or more information elements (as identified below) required for change notifications.

- Seventeen changes do not indicate the type of message: Informational, Authorization, Emergency, or Committee.

- Two changes indicate that changes requiring two approvals will proceed with only one approval unless the requester hears otherwise.

NCUA has not documented and implemented clear and comprehensive change management policies and procedures to ensure that all changes are properly documented and approved. By not having comprehensive documented and implemented change controls for system software, NCUA increases the risk of unauthorized changes being made to NCUA systems. In addition, NCUA's ability to accurately track historical changes is substantially hindered, reducing the ability to identify and reverse any changes later determined to have an adverse impact.

The NCUA Computing Infrastructure System Security Plan requires that all changes to the network be documented by sending an email[3] to the Configuration Control distribution list. Currently, the only exceptions to this rule are changes resulting from an employee add/change/exit action. The email change notification/request must contain six information elements:

1. Type of message.
2. What is this change?

[3] The Configuration Control Mailbox will keep a history of all changes.

3. Why is it needed?
4. When is it planned to be implemented?
5. Who is affected?
6. What is your recovery plan in case of trouble?

In addition, given that all GSS components have a minimum security categorization of Moderate, they are subject to the following requirements per NIST 800-53:

- The organization develops, disseminates, and periodically reviews/updates: (i) a formal, documented, configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

- Configuration change control involves the systematic proposal, justification, implementation, test/evaluation, review, and disposition of changes to the information system, including upgrades and modifications.

- The organization employs automated mechanisms to: (i) document proposed changes to the information system; (ii) notify appropriate approval authorities; (iii) highlight approvals that have not been received in a timely manner; (iv) inhibit change until necessary approvals are received; and (v) document completed changes to the information system.

Recommendation 2: We recommend that OCIO:

1) Update its system software change control policies and procedures.

2) Ensure that all information required for a change request/notification is properly documented.

Agency Response: Agree. OCIO will revisit the system software change control procedures and strengthen them with emphasis on improving the implementation and tracking documentation. This will be implemented by June 1, 2009.

OIG Response: The OIG concurs with the planned corrective actions.

3. NCUA needs to improve its vulnerability management procedures.

This finding pertains to a FY 2007 finding that noted a number of ports/communication services were available on NCUA SAP and ARIES servers. Follow-up from the FY 2007 assessment indicates NCUA management has not implemented a procedure to periodically reassess the number of open ports and services on NCUA servers.

NCUA asserts that, given its current level of resources, it does not have time to periodically reassess the number of open ports and services on NCUA servers. However, by not restricting the number of ports and communication services, NCUA increases the risk of an unauthorized person gaining access to the systems. NCUA should correlate its systems' ports and services to a business need and the services required that meet that business need.

NIST SP 800-53 guides that organizations conduct 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 3: We recommend that OCIO implement a procedure to periodically reassess and determine the business need for the open ports and services on NCUA servers.

Agency Response: Agree. OCIO will implement this recommendation. June 1, 2009 is our projected completion date.

OIG Response: The OIG concurs with the planned corrective action.

4. NCUA has not completed E-Authentication risk assessments[4] for its systems.

While NCUA has completed formal risk assessments for its six NCUA systems, NCUA did not specifically address E-Authentication risk considerations. This is a repeat finding from the FY 2006 and FY 2007 FISMA evaluations. 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 requires agencies to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. Additionally, the guidance 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 4: We recommend OCIO complete the E-Authentication risk assessment process in accordance with OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.

[4] An E-Authentication risk assessment identifies key user roles and transactions within the application; Organizes consequences of false positive authentication and impacts to the agency; and aids in mapping the application to a set of pre-defined authentication criteria by aligning each transaction to a consequence level.

Agency Response: Agree. OCIO will complete the E-Authentication risk assessment by June 1, 2009.

OIG Response: The OIG concurs with the planned corrective action.

5. NCUA has not completed security controls testing for one of its FISMA systems.

NCUA completed testing for five of its six FISMA systems. However, while the NCUA POA&M for FY 2007 indicated security controls testing was considered fully complete, NCUA did not perform security controls testing for the NCUA Accounting System in FY 2007. This is a repeat finding from the FY 2007 FISMA evaluation.

By not performing security controls testing for its systems, NCUA may not know whether security controls in place are operating effectively. This may prevent NCUA from appropriately mitigating risks to an acceptable level, which could adversely impact the security, integrity or availability of its systems.

FISMA requires CIOs to 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 test security controls at least annually.

Recommendation 5: We recommend that OCIO complete security controls testing for its FISMA systems using guidance specified by NIST SP 800-53, *Recommended Security Controls for Federal Information Systems*.

Agency Response: Agree. OCIO will complete security controls testing by September 30, 2008.

OIG Response: The OIG concurs with the planned corrective action.

6. NCUA does not have a formal agency-wide security configuration guide.

NCUA leverages some configuration standards for workstations and servers. However, NCUA has not developed a formal agency-wide security configuration guide that implements a baseline configuration following the NIST enterprise baseline configuration. This is a repeat finding from the FY 2006 and FY 2007 FISMA evaluations.

To date, NCUA has not prioritized the incorporation of NIST standards to develop and implement configuration standards as part of the system development lifecycle and security environment. By not establishing and implementing a formal security configuration guide, the NCUA increases the risk of not consistently applying security standards across agency IT resources. This could expose NCUA systems and sensitive data to threats in a risk-inherent IT environment that is continuously changing.

OMB Memorandum 08-21 indicates FISMA 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. This allows agencies to improve system performance, decrease operating costs, and ensure public confidence in the confidentiality, integrity, and availability of Government information.

Recommendation 6: We recommend that OCIO develop and implement a formal agency-wide security configuration guide that provides a baseline configuration following NIST standards.

Agency Response: Agree. OCIO will strengthen current configuration policy and ensure adequate documentation of these standards. This will be completed by June 1, 2009.

OIG Response: The OIG concurs with the planned corrective action.

7. NCUA has not updated its employee enter/exit/change procedures.

OCIO has formal employee enter/exit/change procedures, which include notification to OCFO, OHR and OCIO staff. However, the procedures are outdated and do not effectively define responsibilities. In addition, the distribution lists for notification of terminated employees includes individuals who are no longer responsible for removing users' access. Furthermore, OCIO has not documented and disseminated a process for removing terminated employees' access from NCUA systems. This is a repeat finding from the FY 2007 FISMA evaluation.

By not having current and effective employee enter/exit/change procedures, NCUA staff who have a role in terminating employees may not receive timely notification and do not fully understand their roles and responsibilities. In addition, by not removing the access of terminated employees, these former employees may retain unauthorized access to sensitive NCUA data and systems. For example, in FY 2006, the OIG investigated and prosecuted a case involving unauthorized access by a former employee whose access had not been removed timely. While OCIO was responsible for the existing enter/exit/change procedures, we believe OHR is the appropriate office for controlling these procedures since they are overall responsible for all employees entering to, exiting from and changing positions within NCUA.

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 employee enters, exits or needs changes to their employee information, the responsible office will email information (where applicable) to the appropriate distribution lists.

NIST SP 800-12, indicates 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 7: We recommend that:

- OHR work with OCIO, OCFO and Regional offices to develop NCUA employee enter/exit/change procedures that will provide a means for NCUA management to enforce timely notification and accountability for all staff involved in the termination process.

- OCIO develop and distribute procedures for removing the system access of terminated employees.

Agency Response: Agree.

- OHR will work with representatives from OCIO, OCFO and the regions to develop and implement employee enter/exit/change procedures in order to enforce timely notification and accountability of all staff changes.
- OCIO will develop and distribute procedures for removing the system access of terminated employees.

OIG Response: The OIG concurs with the planned corrective actions.

8. NCUA lacks a comprehensive contingency planning program for its FISMA systems.

NCUA's contingency planning program does not address key elements recommended for a comprehensive contingency plan. In addition, NCUA Disaster Recovery/System Contingency plans are not:

- Updated periodically.

- Tested on a routine basis (and at least annually).

- Integrated to incorporate all business applications and computing infrastructure.

- Consistently developed for all applications and business processes.

NCUA does not have policies and procedures for system owners for developing, maintaining and testing contingency plans. By not developing, routinely testing and updating its IT system disaster recovery and contingency plans or including all key elements within a documented contingency plan, NCUA cannot ensure its ability to continue operations for information systems that support its operations and assets.

NIST 800-53, guides that information system disaster recovery and contingency plans must be updated frequently, at least annually, and that contingency plan testing is coordinated with other business applications and regional requirements.

Recommendation 8: We recommend that OCIO establish policies and procedures for developing, maintaining and testing disaster recovery and contingency plans, and test and update the plans at least annually.

Agency Response: Agree. OCIO will more adequately document our disaster recovery and contingency plans and more adequately document the testing of these plans. Projected completion date is June 1, 2009.

OIG Response: The OIG concurs with the planned corrective actions.

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

OCIO has not implemented continuing education requirements for its IT employees. While NCUA requires all employees to participate in annual security awareness training and encourages employees to request training needs, OCIO does not define the number of annual training hours IT employees should receive. In addition, we determined OHR does not have a centralized system for managing and tracking employee training records; therefore, training documentation is not readily available. This is a repeat finding from the FY 2007 FISMA evaluation.

By not defining a training requirement program and requiring IT employees to take security related training, NCUA cannot ensure its IT employees 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 indicates that training oversight includes general awareness training and specific training for people with significant security responsibilities. The policy requires the CIO to ensure adequate training is planned for NCUA.

NIST SP 800-53 guides that organizations provide system managers, system and network administrators, and other personnel having access to system-level software with adequate technical training to perform their assigned duties. It also guides that the organization document and monitor individual information system security training activities including basic security awareness training and specific information system security training.

Recommendation 9: We recommend that:

1) OCIO establish continuing education requirements for IT employees.

2) OHR implement a mechanism to effectively track and report training taken.

Agency Response: Agree.

- Each OCIO division director will establish continuing education requirements for their employees and document this training using the Individual Development Plan (IDP)[5] system.
- OHR has issued a request-for-proposals to contract for a web-based learning management system (LMS). The LMS will enable the Office to monitor and track training records for every employee. OHR projects the LMS will be operational by April 2009.

OIG Response: The OIG concurs with the planned corrective actions.

10. NCUA needs to improve its Plans of Action and Milestones (POA&M) process.

While NCUA has taken some steps to correct prior year findings, six previously identified deficiencies still remain. To correct these remaining actions, NCUA needs to:

- Complete its E-Authentication risk assessments.
- Define continuing education requirements and establish a mechanism to effectively track and report employees' training taken
- Update employee enter/exit/change procedures.
- Implement a procedure to periodically reassess the number of open ports and services on NCUA servers.
- Develop an agency-wide security configuration guide.
- Complete security controls testing for NAS.

NCUA does not sufficiently review and validate whether program officials fully remediate weaknesses identified in the POA&M prior to marking the item as "completed." Therefore, NCUA does not properly address and resolve weaknesses identified in the POA&M, which reduces NCUA's level of compliance with OMB requirements. This could ultimately reduce NCUA's ability to provide confidentiality, integrity, and availability of data within FISMA systems.

[5] An IDP ensures that employees maintain the current level of job proficiency through continued training and developmental activities. In addition, employees identify new knowledge, skills and abilities to pursue, as well as learning activities needed to reach the established goals.

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. The POA&M process is intended to be a tool for program officials to note changes and updates, usually on a quarterly basis.

Recommendation 10: We recommend that NCUA update its procedures to ensure POA&M items are complete.

Agency Response: Agree. OCIO will update our procedures to require the Deputy CIO to sign off on completed items. Implementation is immediate.

OIG Response: The OIG concurs with the planned corrective action.