NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

OIG REPORT TO OMB ON THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT 2005

Report #OIG-05-08 **September 30, 2005**

William A. DeSarno
Inspector General

Released by:

James Hagen
Asst IG for Audits

Auditor-in-Charge:

Tammy F. Rapp, CPA, CISA
Sr Information Technology Auditor

OIG REPORT TO OMB ON THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY ACT - 2005
Report #OIG-05-08

CONTENTS

Appendices are limited to restricted official use only.

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged Cotton & Company LLP to conduct an independent evaluation of 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.

Cotton & Company 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 scheduled an exit conference with NCUA officials on October 3, 2005, to discuss evaluation results, but the OCIO respectfully declined.

Our work identified two issues that can be classified as significant deficiencies in NCUA's security structure. OMB defined a significant deficiency for FISMA reporting purposes in its 2004 reporting guidance (OMB M-04-25):

> *Significant Deficiency – is a weakness in an agency's overall information systems security program or management control structure, or within one or more information systems, that significantly restricts the capability of the agency to carry out its mission or compromises the security of its information, information systems, personnel, or other resources, operations, or assets. In this context, the risk is great enough that the agency head and outside agencies must be notified and immediate or near-immediate corrective action must be taken.*

While the Chief Information Officer (CIO) has initiated projects to address these issues, both of the significant deficiencies concerning NCUA's security program remain open and are being reported for the third consecutive year.

First, this year and in prior-year reviews we noted several weaknesses related to NCUA's General Support System (GSS) Certification and Accreditation (C&A) and its technical components. This is significant, because every major application relies on the security of the operating system and network infrastructure on which it resides. Prevention of unauthorized access is necessary to ensure infrastructure security. NCUA's general support system continues to operate under an interim accreditation based on several weaknesses identified during the formal certification process in 2004.

In response to this issue, the CIO has initiated a project to make major changes to the GSS and upgrade a number of its components. As of the end date of our fieldwork, the GSS is still undergoing the change process, and the C&A of the new GSS had not been completed. The CIO has, however, brought in an experienced contractor to assist with the C&A activities and ensure that they meet requirements of NIST SP 800-37, *Guide for the Security Certification and Accreditation of Federal Information Systems,* and other federal guidance. This issue remains open and has been expanded to include other weaknesses in the overall C&A process used to review all major systems. This weakness represents a significant deficiency in NCUA's security program.

Second, we determined during prior reviews that information stored on examiners' laptop computers had not been addressed as part of NCUA's information security program. The OCIO recently upgraded the examination application which includes requiring all examination data stored on laptops to be encrypted. When completed, this project will represent an improvement in the protection of sensitive data. Training and implementation for this project will not be completed until November 1, 2005. Therefore, we were not able to test the effectiveness of the program as part of the 2005 review.

We also noted other weaknesses in IT security controls that did not rise to the level of significant deficiencies:

- NCUA has not conducted adequate security control testing of all major information systems on an annual basis.
- Continuity of Operations Plan (COOP) and IT Disaster Recovery procedures do not reflect the current environment and have not been tested in 2005.
- NCUA has not developed policies and procedures for monitoring the security of outsourced systems.
- NCUA does not have a system inventory for all major information systems.
- NCUA has not completed the e-authentication risk assessment for major systems.
- NCUA has not documented policies and procedures guiding the process for managing the Plan of Action and Milestones (POA&M).
- NCUA does not have a configuration management plan that covers all agency systems and has not developed a minimum security baseline configuration for any of its systems or platforms.
- NCUA has not provided security awareness training to employees in 2005.
- NCUA has not conducted privacy impact assessments for any major information systems.

We concluded that these two significant deficiencies remain open after 3 years and other security issues exist, because OCIO management had not created a tone at the top that emphasizes both external perimeter and internal security and security-related activities. Management has placed its focus on external security issues, and internal security has not been made a priority. Management has not dedicated the resources to completing C&As and other security assessments in accordance with FISMA, NIST, and OMB guidance. We encourage NCUA's Executive Director, the Director of the Office of Examination and Insurance, and the CIO to address these issues as soon as possible.