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 2008

Report #OIG-08-07 September 24, 2008

William A. DeSarno
Inspector General

Released by:

James Hagen
Asst IG for Audits

Auditor-in-Charge:

W. Marvin Stith, CISA
Sr Information Technology Auditor

OIG REPORT TO OMB ON THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT - 2008
Report #OIG-08-07

CONTENTS

Appendix A is Audit Report OIG-08-08 dated September 24, 2008.

Section II and Appendix B are limited to restricted official use only.

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.