

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
2007

Report #OIG-07-08 September 12, 2007



A handwritten signature in black ink, reading "William A. DeSarno".

William A. DeSarno
Inspector General

Released by:

A handwritten signature in black ink, reading "James Hagen".

James Hagen
Asst IG for Audits

Auditor-in-Charge:

A handwritten signature in black ink, reading "W. Marvin Stith".

W. Marvin Stith, CISA
Sr Information Technology Auditor

**INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION
INFORMATION SECURITY PROGRAM - 2007
Report #OIG-07-08**

CONTENTS

Section	Page
I EXECUTIVE SUMMARY	1
II OFFICE OF MANAGEMENT & BUDGET REPORT FORMAT	2
Appendix	
A Independent Evaluation of the NCUA Information Security Program – 2007	
B NCUA Financial Statement Audits – FY2006	

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

Appendix A is Audit Report OIG-07-09 dated September 12, 2007.

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.