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 2006

Report #OIG-06-06 September 29, 2006

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

LIMITED OFFICIAL USE ONLY

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 Grant Thornton 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.

Grant Thornton evaluated NCUA's security program through interviews, documentation reviews, 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 Federal Information Processing Standards (FIPS), and Office of Management and Budget (OMB) memorandums. We conducted an exit conference with NCUA officials on September 6, 2006, to discuss evaluation results.

The NCUA made noticeable progress in strengthening its Information Technology (IT) security program during Fiscal Year (FY) 2006. Notable accomplishments include:

- Significant strides in remediation of the significant deficiency noted in the FY2005 report by deploying encryption software to improve security of information stored on examiners' laptop computers, and
- Completion of the Accreditation package for the NCUA General Support System (GSS).

While NCUA has made commendable progress in eliminating the significant deficiencies reported last year, our review this year identified the following weaknesses in IT security controls that deserve immediate management attention:

- Procedures requiring the use of cryptographic security measures for sensitive financial and Personally Identifiable Information (PII) need better enforcement, and Privacy Impact Assessments (PIA) for its systems needs to be developed.

- Certification and accreditation (C&A) of all NCUA systems needs to be completed.

- Password and user account security configurations need improvement, including regular user account reconciliations.

- Personnel security awareness training program needs to be fully implemented.

We also noted the following other weaknesses in IT security controls that management should consider:

- Security planning documentation needs improvement in consistent version control, revisions/updates, and dissemination to required officials.

- E-Authentication risk assessments should be developed for NCUA's systems.

- Security configuration guides need to be developed.

- Continuity of Operations Plan (COOP) and Disaster Recovery procedures need to be more consistently updated and tested including the regular testing of NCUA's Disaster

Recovery and system contingency plans. In addition, restoration priorities related to system impact ratings need to be consistently applied and documented.

- Physical security measures need to be consistently enforced.
- Regular incident response training needs to be conducted.
- NCUA's Plan of Actions and Milestones (POA&M) process needs improvement.

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

.