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 2004

Report #OIG-04-06 **September 30, 2004**

Herbert S. Yolles
Inspector General

Released By:

William A. DeSarno
Deputy Inspector General for Audits

Auditor-in-Charge:

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

TABLE OF CONTENTS

Note: Exhibits transmittal separately and restricted for 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 NCUA's information systems (IS) and security program and controls for compliance with the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002.

The Office of Management & Budget (OMB) issued 2004 Guidance on Annual Information Technology Security Reports on August 23, 2004. This guidance provides clarification to agencies for implementing, meeting, and reporting FISMA requirements to OMB and the Congress. This report contains a summary of our evaluation of the NCUA's information security program and is presented in the OMB prescribed format.

The OIG issued two reports during the past year that reported on the testing of the effectiveness of information security and internal controls:

- On September 30, 2004, the OIG issued a report containing an Independent Evaluation of the NCUA's Information Security Program – 2004. The content of the independent evaluation report supports the conclusions presented in this report. Refer to Exhibit A for the complete independent evaluation.

- On March 31, 2004, the OIG issued the Financial Statement Audit Report for the year ended December 31, 2003. The purpose of this audit was to express an opinion on whether the financial statements were fairly presented. In addition, the internal control structure was reviewed and an evaluation of compliance with laws and regulations was performed as part of the audit. The result of this audit was an unqualified opinion, stating that the financial statements were presented fairly. Although there were no material weaknesses identified during the review of the internal control structures pertinent to financial report, nine recommendations were made relating to weaknesses in the area of information security. Refer to Exhibit B for the Information Technology Controls Review report.

The Chief Information Officer (CIO) has made progress during the past year to improve NCUA's IT infrastructure. During 2004, NCUA accomplished the following:

- Completed an interim certification and accreditation of their general support system;
- Completed and updated several security plans and risk assessments; and
- Identified and reported 114 weaknesses in the NCUA Plans of Action and Milestones (POA&M) report. Of the 114 items, 60 were completed, 38 have milestones or completion dates that are due after the FISMA report date, 8 were delayed, the OCIO made risk based decisions to accept risk on 6, and 2 were identified as significant deficiencies for this year's FISMA reporting cycle.

However, two significant deficiencies concerning NCUA's security program carried over from last year's independent evaluation still have not been fully addressed. First, we determined that information stored on examiners' laptop computers has not been addressed as part of NCUA's information security program. We've noted that NCUA has taken some measures to protect information on examiners laptops. However, a formal review of the risks involved and protections necessary to address these risks has not been conducted. This could result in the intentional or accidental release of credit union member information.

Second, we noted several weaknesses related to the underlying general support systems and network components. This is significant because every 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. Therefore if the underlying operating systems and network components are not secure, then the applications themselves cannot be assured of being secure. NCUA's general support system is operating under an interim accreditation based on several weaknesses identified during the formal certification process. As of the ending date of fieldwork, the general support system is operating at medium to high risk because NCUA has not corrected or accepted risk on weaknesses identified during the interim certification.

While we noted other weaknesses in IT controls, we concluded the two conditions described above are the most significant to NCUA. Additionally, both of these conditions were reported in last year's FISMA review as material weaknesses. 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.