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 2003

Report #OIG-03-07 **September 12, 2003**

Herbert S. Yolles

Herbert S. Yolles
Inspector General

Released By:

William A. DeSarno

William A. DeSarno
Deputy Inspector General for Audits

Auditor-in-Charge:

Tammy F. Rapp

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

TABLE OF CONTENTS

Section **Page**

Exhibits

Note: Exhibits transmitted separately and restricted for official use only.

I. SUMMARY OF RESULTS

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 security program and controls for compliance with the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002, and Office of Management and Budget (OMB) Circular A-130, Appendix III.

The OMB issued Fiscal Year 2003 Guidance on Annual Information Technology Security Reports on August 7, 2003. This guidance provided 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 March 31, 2003, the OIG issued the Financial Statement Audit Report for the year ended December 31, 2002. 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 reporting, eight recommendations were made relating to weaknesses in the area of information security. Refer to Exhibit B for the Executive Summary, Observations and Recommendations, and Detailed Information Technology Observations sections of this report.

- On September 12, 2003, the OIG issued a report containing an Independent Evaluation of the NCUA's Information Security Program - 2003. The content of the independent evaluation report supports the conclusions presented in this report. Refer to Exhibit A for the complete independent evaluation.

The Chief Information Officer (CIO) is to be commended for the actions taken to improve NCUA's information technology (IT) infrastructure. During FY2003, NCUA accomplished the following:

- Completed certification of eight systems
- Completed and updated several security plans.

Even with these efforts, the independent evaluation identified significant weaknesses with the base structure of NCUA's security program that impacts the security of all information residing on the network. Overall, the evaluation determined that NCUA's information security program does not fully meet the minimum security requirements of the Office of Management and Budget Circular A-130, *Management of Federal Resources*, Appendix III, *Security of Federal Automated Information Resources*. Two significant deficiencies exist in the NCUA IT infrastructure.

First, we noted several weaknesses related to the underlying general support systems and network. This is significant because every application relies on the security of the operating system on which it resides. Therefore if the underlying operating systems are not secure, then the applications themselves cannot be assured of being secure.

Second, we determined that information stored on examiners' laptop computers is not adequately secured. Examiners frequently store credit union member personal financial information (credit union share and loan "downloads") on their laptop computers. We noted during our review that the examiner laptops and the information stored on the laptops were not considered in any system security plan or certification and accreditation document. In our judgment, this information is quite sensitive and presents a significant security risk. While we recognize that the likelihood of a security breach involving this information is uncertain, the potential damage to credit unions and their members and to NCUA's reputation is quite significant. Accordingly, we believe that any subsequent security plan or certification and accreditation document should consider adequate safeguards for this information.

While we noted other significant weaknesses in IT controls, we believe that the two conditions described above are the most significant to NCUA, and should be addressed as soon as possible by NCUA's Executive Director and CIO.

In October 2002, the CIO identified and reported 167 weaknesses to OMB in the NCUA's Plans of Action and Milestones (POA&M) report. Additionally, the independent evaluation supporting this report identified 12 new weaknesses and made specific recommendations to address those weaknesses. The table below shows the current status of the weaknesses, along with the new recommendations identified in the independent evaluation.

Description	Number of Weaknesses
Reported in NCUA's FY 2002 POA&M	167
Completed/Implemented Fully During FY 2003	45*
Partially Completed/Implemented	46
New Weaknesses	12
FY 2002 Weaknesses Awaiting Implementation	76
As of August, 2003	

* Although OCIO reported 148 of the 165 weaknesses had been corrected in its July 1, 2003, letter to OMB, we obtained documentation supporting only 45 corrective actions completed.

II. OFFICE OF MANAGEMENT & BUDGET REPORT FORMAT

A. Overview of FISMA IT Security Reviews

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate.

A.1. Identify the agency's total IT security spending and each individual major operating division or bureau's IT security spending as found in the agency's FY03 budget enacted. This should include critical infrastructure protection costs that apply to the protection of government operations and assets. Do not include funding for critical infrastructure protection pertaining to lead agency responsibilities such as outreach to industry and the public.	
Bureau Name	**FY03 IT Security Spending ($ in thousnds)**
National Credit Union Administration (NCUA)	N/A - OIG response not required
Agency Total	

A.2a. Identify the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials and CIOs in FY03, the total number of contractor operations or facilities, and the number of contractor operations or facilities reviewed in FY03. Additionally, IGs shall also identify the total number of programs, systems, and contractor operations or facilities that they evaluated in FY03.						
	FY03 Programs		**FY03 Systems**		**FY03 Contractor Operations or Facilities**	
Bureau Name	Total Number	Number Reviewed	Total Number	Number Reviewed	Total Number	Number Reviewed
NCUA	1	0	13	12*	4	4
Agency Total	1	0	13	12	4	4
b. For operations and assets under their control, have agency program officials and the agency CIO used appropriate methods (e.g., audits or inspections, agreed upon IT security requirements for contractor provided services or services provided by other agencies) to ensure that contractor provided services or services provided by another agency for their program and systems are adequately secure and meet the requirements of FISMA, OMB policy and NIST guidelines, national security policy, and agency policy?	Yes			No		X
c. If yes, what methods are used? If no, please explain why.	Sufficient due diligence was not performed to ensure services provided by a payroll/personnel contract agency were adequately secure.					
d. Did the agency use the NIST self-assessment guide to conduct its reviews?	Yes		X	No		
e. If the agency did not use the NIST self-assessment guide and instead used an agency developed methodology, please confirm that all elements of the NIST guide were addressed in the agency methodology.	Yes			No		
f. Provide a brief update on the agency's work to develop an inventory of major IT systems.	NCUA is considering adding two systems to its inventory: Travel Mgmt System and Corporate Exam System.					

* The OCIO reviewed all systems except the infrastructure and 5300. As part of the independent evaluation, the OIG reviewed the infrastructure, 5310, TAPS, CHRIS, and ESS. SAP, CLF, and CDRLF were reviewed as part of the financial statement audit.

A.3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law in FY03. Identify the number of material weaknesses repeated from FY02, describe each material weakness, and indicate whether POA&Ms have been developed for all of the material weaknesses.

	FY03 Material Weaknesses			
Bureau Name	Total Number	Total Number Repeated from FY02	Identify and Describe Each Material Weakness	POA&Ms developed? Y/N
NCUA	2	1	Network not certified	Y
			Sensitive credit union member data needs better protection	N
Agency Total				

A.4. This question is for IGs only. Please assess whether the agency has developed, implemented, and is managing an agency-wide plan of action and milestone process that meets the criteria below. Where appropriate, please include additional explanation in the column next to each criteria.	**Yes**	**No**
Agency program officials develop, implement, and manage POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	X	
Agency program officials report to the CIO on a regular basis (at least quarterly) on their remediation progress.	X	
Agency CIO develops, implements, and manages POA&Ms for every system that they own and operate (systems that support their programs) that has an IT security weakness.	X	
The agency CIO centrally tracks and maintains all POA&M activities on at least a quarterly basis.	X	
The POA&M is the authoritative agency and IG management tool to identify and monitor agency actions for correcting information and IT security weaknesses.	X	
System-level POA&Ms are tied directly to the system budget request through the IT business case as required in OMB budget guidance (Circular A-11) to tie the justification for IT security funds to the budget process.	N/A	
Agency IGs are an integral part of the POA&M process and have access to agency POA&Ms.	X	
The agency's POA&M process represents a prioritization of agency IT security weaknesses that ensures that significant IT security weaknesses are addressed in a timely manner and receive, where necessary, appropriate resources.		X

Although NCUA tracks security weaknesses using the POAM, the POAM process needs to be better managed:

- Recommendations found in the POAM were not prioritized.
- Documentation was not available to demonstrate implementation of recommendations.
- The POAM indicated some recommendations were implemented where risk based decisions were made to not implement the recommendation.

B. Responsibilities of Agency Head

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to the following questions:

B.1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth FISMA's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced?	NCUA Instruction 13500.4, dated Feb 21, 2002, delegates security authority to the CIO and respective designees.
B.2. Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?	Although managers have discretionary budget authority over their respective operations, the final integration of systems is approved by the CIO.
B.3. How does the head of the agency ensure that the agency's information security plan is practiced throughout the life cycle of each agency system?	The Executive Director (ED) delegated the oversight of the security program to the Deputy ED.
B.4. During the reporting period, did the agency head take any specific and direct actions to oversee the performance of 1) agency program officials and 2) the CIO to verify that such officials are ensuring that security plans are up-to-date and practiced throughout the lifecycle of each system? Please describe.	Although the CIO reports to the Executive Director (ED) on IT matters, the ED has not developed a specific requirement for the CIO or program officials to report on the effectiveness of the security program.
B.5. Has the agency integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., continuity of operations, and physical and operational security)? Please describe.	NCUA does not have any critical infrastructure responsibilities. Although NCUA has coordinated physical security with the Div of Procurement and Facilities, we made recommendations for improvement.
B.6. Does the agency have separate staffs devoted to other security programs, are such programs under the authority of different agency officials, if so what specific efforts have been taken by the agency head or other officials to eliminate unnecessary duplication of overhead costs and ensure that policies and procedures are consistent and complimentary across the various programs and disciplines?	Since NCUA is a small agency, there is only one position, the Information Security Officer, dedicated full-time to the information security program. The Div of Procurement and Facilities has responsibility for physical security and coordinates with the OCIO.

B.7. Identification of agency's critical operations and assets (both national critical operations and assets and mission critical) and the interdependencies and interrelationships of those operations and assets.				
a. Has the agency fully identified its national critical operations and assets?	Yes	N/A	No	N/A
b. Has the agency fully identified the interdependencies and interrelationships of those nationally critical operations and assets?	Yes	N/A	No	N/A
c. Has the agency fully identified its mission critical operations and assets?	Yes		No	X
d. Has the agency fully identified the interdependencies and interrelationships of those mission critical operations and assets?	Yes		No	X
e. If yes, describe the steps the agency has taken as a result of the review.				
f. If no, please explain why.	The ISO plans to perform a review of mission critical systems and interrelationships during the next year.			

B.8. How does the agency head ensure that the agency, including all components, has documented procedures for reporting security incidents and sharing information regarding common vulnerabilities?				
a. Identify and describe the procedures for external reporting to law enforcement authorities and to the Federal Computer Incident Response Center (FedCIRC).	The ISO has responsibility for communicating incidents to FedCIRC.			
b. Total number of agency components or bureaus.	1			
c. Number of agency components with incident handling and response capability.	1			
d. Number of agency components that report to FedCIRC.	1			
e. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	Y			
f. What is the required average time to report to the agency and FedCIRC following an incident?	24 hours			
g. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	OCIO does not have a policy regarding patches. OCIO activated Qualys to identify patches, configuration problems, and known vulnerabilities.			
h. Is the agency a member of the Patch Authentication and Distribution Capability operated by FedCIRC?	Yes	X	No	
i. If yes, how many active users does the agency have for this service?	1 - The ISO			
j. Has the agency developed and complied with specific configuration requirements that meet their own needs?	Yes		No	X
k. Do these configuration requirements address patching of security vulnerabilities?	Yes		No	X

B.9. Identify by bureau, the number of incidents (e.g., successful and unsuccessful network penetrations, root or user account compromises, denial of service attacks, website defacing attacks, malicious code and virus, probes and scans, password access) reported and those reported to FedCIRC or law enforcement.			
Bureau Name	Number of incidents reported	Number of incidents reported externally to FedCIRC	Number of incidents reported externally to law enforcement
NCUA	1	1	1

C. Responsibilities of Agency Program Officials and Agency Chief Information Officers

In this section, the agency must respond to performance measures and may provide narrative responses where appropriate to identify and describe the performance of agency program officials and the agency CIO in fulfilling their IT security responsibilities.

C.1. Have agency program officials and the agency CIO: 1) assessed the risk to operations and assets under their control; 2) determined the level of security appropriate to protect such operations and assets; 3) maintained an up-to-date security plan (that is practiced throughout the life cycle) for each system supporting the operations and assets under their control; and 4) tested and evaluated security controls and techniques? By each major agency component and aggregated into an agency total, identify actual performance in FY03 according to the measures and in the format provided below for the number and percentage of total systems.

a. Bureau Name	b. Total Number of Systems	c. Number of systems assessed for risk and assigned a level or risk		d. Number of systems that have an up-to-date IT security plan		e. Number of systems certified and accredited		f. Number of systems with security control costs integrated into the life cycle of the system		g. Number of systems for which security controls have been tested and evaluated in the last year		h. Number of systems with a contingency plan		i. Number of systems for which contingency plans have been tested	
		No. of Systems	% of Systems	No.	%	No.	%	No.	%	No.	%	No.	%	No.	%
NCUA	13	11	85%	11	85%	8	62%	13	100%	11	85%	12	92%	1	8%
Agency Total	**13**	**11**	**85%**	**11**	**85%**	**8**	**62%**	**13**	**100%**	**11**	**85%**	**12**	**92%**	**1**	**8%**

Some of the above statistics are based on input from the ISO and have not been verified. As part of the independent evaluation and OIG rotational review of systems, the infrastructure and four applications were reviewed during 2003.

C.2. Identify whether the agency CIO has adequately maintained an agency-wide IT security program and ensured the effective implementation of the program and evaluated the performance of major agency components.

Has the agency CIO maintained an agency-wide IT security program? Y/N	Did the CIO evaluate the performance of all agency bureaus/components? Y/N	How does the agency CIO ensure that bureaus comply with the agency-wide IT security program?	Has the agency CIO appointed a senior agency information security officer per the requirements in FISMA?	Do agency POA&Ms account for all known agency security weaknesses including all components?
N	N	Delegation to the ISO	Y	N

Although the CIO developed an agency-wide security program, it has not been updated during the past year to reflect changes in the infrastructure or security weaknesses identified. In addition, the CIO has not certified its infrastructure or the 5300 system.

The agency POAMs were not updated to reflect IT security weaknesses identified during the financial statement audit. In addition, the ISO plans to include weaknesses recently identified during the certification process in the October 2003 POAM.

C.3. Has the agency CIO ensured security training and awareness of all agency employees, including contractors and those employees with significant IT security responsibilities?

Total number of agency employees in FY03	Agency employees that received IT security training in FY03		Total number of agency employees with significant IT security responsibilities	Agency employees with significant security responsibilities that received specialized training		Briefly describe training provided	Total costs for providing training in FY03
	Number	Percentage		Number	Percentage		
963	230	24%	18	11	61%	Conferences and in-house training	$4,810

The above statistics were provided by the ISO and have not been verified. However, the OIG attended training presented by the CIO that included security aspects related to new notebooks distributed in early 2003.

C.4. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were IT security requirements and costs reported on every FY05 business case (as well as in the exhibit 53) submitted by the agency to OMB?

Bureau Name	Number of business cases submitted to OMB in FY05	Did the agency program official plan and budget for IT security and integrate security into all of their business cases? Y/N	Did the agency CIO plan and budget for IT security and integrate security into all of their business cases? Y/N	Are IT security costs reported in the agency's exhibit 53 for each IT investment? Y/N
NCUA	N/A	N/A	N/A	N/A

Although NCUA is not required to complete a capital asset plan with its budget submission to OMB, NCUA intends to incorporate security with its strategic plan and enterprise architecture. Since a significant portion of NCUA's information security is handled by the infrastructure, NCUA has not taken any steps to integrate security funding at the system level.