NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

OIG REPORT TO OMB
ON NCUA COMPLIANCE WITH
GOVERNMENT INFORMATION
SECURITY REFORM ACT
2002

Report #OIG-02-12 **September 16, 2002**

Acting Inspector General:

William A. DeSarno

Auditor in Charge:

Tammy F. Rapp, CPA

h

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
OIG REPORT TO OMB ON NCUA COMPLIANCE WITH GOVERNMENT INFORMATION SECURITY REFORM ACT 2002

EXECUTIVE SUMMARY

The Government Information Security Reform Act (GISRA), Public Law 106-398, requires Inspectors General (IG) to perform independent evaluations to:

- Assess compliance with GISRA and agency security policies and procedures; and
- Test effectiveness of information security control techniques for a subset of the agency's information systems.

The NCUA OIG performed three reviews during the reporting cycle that tested effectiveness of information security and internal controls:

- On March 7, 2002, the OIG issued a report containing an Evaluation of Project Risks Associated with an Upgrade to Comprehensive Human Resources Integrated System (CHRIS). The purpose of our review was to determine whether NCUA had mitigated the project risks of a major HR system upgrade by performing appropriate analysis, planning, and monitoring. The focus of this review was intended to provide reasonable assurance regarding the design and effectiveness of controls over systems and procedures. Our review identified several system migration weaknesses. We reported that these weaknesses could lead to overall increased project risk, NCUA needs/requirements not being met, the planned implementation timeframe not being met, increased security and system access risks, and expanding costs. According to NCUA, the conversion was successfully completed in Spring 2002.

- On March 31, 2002, the OIG issued the Financial Statement Audit Report for the year ended December 31, 2001. 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, eighteen recommendations were made relating to weaknesses in the area of information security.

- On September 16, 2002, the OIG issued a report containing an evaluation of NCUA's compliance with the Government Information Security Reform Act. Although NCUA has not achieved full compliance with GISRA, the agency has made significant progress toward that goal. NCUA has established the basis for an improved information security program, which if properly implemented and

maintained over time should meet the goals set forth by GISRA. NCUA has appointed a Security Officer to oversee the security program. During the past year, the Security Officer has coordinated the completion of risk assessments and security plans for most of NCUA's systems. In addition, NCUA has made acceptable progress in correcting information security issues previously identified in other reviews.

The overall objective of this review was to perform an independent evaluation as required by GISRA in order to assess compliance with GISRA and agency security policies and procedures. To fulfill the objectives of the review, we performed a detailed review of NCUA's risk assessments, security plans, and other relevant documents where available. In addition, we interviewed each of the designated systems business owners in order to execute a compliance gap analysis for each of the major computer systems. The procedures also included reviewing available documentation to determine:

- The level of compliance for each of the critical elements under review;
- Items requiring a corrective action plan; and
- Accepted risks associated with each system.

The NCUA Office of Inspector General (OIG) determined that NCUA is actively working towards compliance with GISRA. The following represents the agency's status toward compliance with key GISRA provisions as of August 2002:

- NCUA established policies and procedures for an agency-wide security program. In February 2002, the Executive Director issued an instruction to all staff outlining the security responsibilities of the CIO, Offices of Primary Interest, and Information Security Officer. NCUA also prepared a document with Information Security Procedures. The goal of this document is to establish the procedures used by NCUA to create and maintain an agency-wide security plan. This plan will provide the basis for a high-level oversight of all security efforts, ensure that all security measures are well coordinated, and will provide an operating framework for all more specific security plans.

- NCUA is in the process of updating its Continuity of Operations Plan. In addition, the disaster recovery plan was tested successfully. Although the infrastructure disaster recovery plan covers the recoverability of the systems, business owners have not documented a business continuity plan for processes supported by their systems. Most of the system owners verbally communicated to us the steps they would take should their system become unavailable; however, these processes are not documented for someone other than the business owner to carry out.

- The CIO and Information Security Officer had oversight over the agency-wide security program and ensured effective implementation by working with program officials. The CIO and Security Officer assisted agency program officials with their risk assessments and security plans.

- The CIO contracted with an independent public accounting firm to perform a penetration test. The results of the penetration test did not reveal any material security weaknesses.

- NCUA program officials performed risk assessments on eighteen systems, plus an additional system's risk assessment was performed subsequent to our review.

- NCUA program officials developed eighteen security plans for each system they under their control, and one additional system's security plan was developed subsequent to our review.

- NCUA program officials need to perform periodic management testing of controls for their systems as required by GISRA.

- NCUA needs to perform due diligence reviews to ensure adequate security steps have been taken for systems and services provided by other government agencies and contractors.

- For the reporting cycle, NCUA provided security training to personnel with significant security responsibilities. Security awareness training was provided to most employees during a bi-annual regional conference sponsored by NCUA. In addition, new examiners are provided with basic computer training, which includes security awareness. NCUA plans to use their video taped regional conference presentation for contractors and new non-examiner personnel.

- A formal incident response capability has been documented, but still needs to be implemented.

- NCUA plans to develop and implement an intrusion detection system by the end of 2002.

The OIG made specific recommendations to management that address concerns identified during this review.

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
OIG REPORT TO OMB ON NCUA COMPLIANCE WITH GOVERNMENT INFORMATION SECURITY REFORM ACT 2002

OMB QUESTIONS with OIG RESPONSE

The Office of Management and Budget (OMB) has requested OIGs to submit the results of their independent evaluation by responding specifically to questions in OMB Memorandum M-02-09. The following presents our evaluation of the National Credit Union Administration's (NCUA) compliance with GISRA. While the OCIO shared its preliminary draft report to OMB with the OIG, there was insufficient time to verify the content of the agency's submission to OMB.

A. General Overview

1. Identify the agency's total security funding as found in the agency's FY02 budget request, FY02 budget enacted, and the President's FY03 budget.

   No OIG evaluation required.

2. Identify and describe as necessary the total number of programs and systems in the agency, the total number of systems and programs reviewed by the program officials, CIOs, or IGs in both last year's report (FY01) and this year's report (FY02) according to the format provided below. Agencies should specify whether they used the NIST self-assessment guide or an agency developed methodology. If the latter was used, confirm that all elements of the NIST guide were addressed.

   During 2001, NCUA did not identify programs for this purpose. NCUA identified seven mission critical systems that did not include other critical systems that were maintained by other agencies such as the agency's personnel processing system, payroll system, time and attendance system, and disbursement system. NCUA's program officials and CIO did not perform any program reviews during 2001. The OIG performed two independent evaluations that included information security and internal controls during the 2001 reporting period: SAP Security Review and 2000 Financial Statement Audits. Both independent evaluations included NCUA's core financial system, which is one of the agency's mission critical systems.

   During 2002, NCUA determined there is one program supported by nineteen systems, which include the systems that were left out of the 2001 GISRA reporting cycle. Program officials and the CIO prepared eighteen security plans and performed eighteen risk assessments using NIST SP 800-26. The CIO contracted with an independent public accounting firm to perform a penetration test, which disclosed no material weaknesses. However, program officials have not independently tested or validated security controls over their respective systems.

During the 2002 reporting period, the OIG performed three independent evaluations that evaluated information security and internal controls: 2001 Financial Statement Audits, Evaluation of Project Risks Associated with Upgrade to Comprehensive Human Resources Integrated System, and Independent Evaluation of NCUA's Information Security Program.

	FY01	FY02
a. Total number of agency programs.	*0*	*1*
b. Total number of agency systems.	*7*	*19*
c. Total number of programs reviewed.	*0*	*0*
d. Total number of systems reviewed.	*1*	*4*

3. Identify all material weakness in policies, procedures, or practices as identified and required to be reported under existing law. (Section 3534(c)(1)-(2) of the Security Act.) Identify the number of reported material weaknesses for FY 01 and FY 02, and the number of repeat weaknesses in FY02.

	FY01	FY02
a. Number of material weaknesses reported.	*0*	*0*
b. Number of material weaknesses repeated in FY02.	*0*	*0*

B. Responsibilities of Agency Head

1. Identify and describe any specific steps taken by the agency head to clearly and unambiguously set forth the Security Act's responsibilities and authorities for the agency CIO and program officials. Specifically how are such steps implemented and enforced? Can a major operating component of the agency make an IT investment decision without review by and concurrence of the agency CIO?

In February 2002, the Executive Director issued an instruction to all staff outlining the security responsibilities of the CIO, Offices of Primary Interest, and Information Security Officer. NCUA also drafted a document with Information Security Procedures. The goal of this document is to establish the procedures used by NCUA to create and maintain an agency-wide security plan. This plan will provide the basis for a high-level oversight of all security efforts, ensure that all security measures are well coordinated, and will provide an operating framework for all more specific security plans.

The CIO and Deputy Executive Director (DED) met periodically throughout the year to discuss progress with GISRA compliance.

Although business managers have discretionary budget authority over their respective operations, the final integration of systems at NCUA is monitored and approved by the CIO. In addition, major acquisitions are evaluated and monitored by the Information Technology Oversight Committee for the strategic integration into NCUA's enterprise architecture.

2. 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? (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.) 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?

   In February 2002, the Executive Director issued an instruction to all staff outlining the security responsibilities of the CIO, Offices of Primary Interest, and Information Security Officer. The agency head delegated the oversight of the agency's security program to the DED who was periodically briefed by the CIO on the progress of the agency's information security program and the implementation of security plans throughout the lifecycle of each system.

   In addition, results from independent reviews and audits are communicated to the Office of the Executive Director (OED). The DED is the agency's audit follow-up official whose responsibility is to ensure that appropriate corrective action is taken on findings.

3. How 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)? (Sections 3534 (a)(1)(B) and (b)(1) of the Security Act.) 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?

Although NCUA does not have any critical infrastructure protection responsibility, NCUA integrated most of its security responsibilities in the agency-wide information technology security program. However, the physical security program requires integration into the overall security program at NCUA.

Since NCUA is a small agency, there is only one individual with responsibility for the agency information security program that reports exclusively to the CIO. There is no additional staff devoted solely to the security program.

4. Has the agency undergone a Project Matrix review? If so, describe the steps the agency has taken as a result of the review. If no, describe how the agency identifies its critical operations and assets, their interdependencies and interrelationships, and how they secure those operations and assets. (Sections 3535(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

   NCUA was not required to undergo a Project Matrix review. However, NCUA management identified systems as those that are supported by OCIO and/or used to support agency operations. Of these nineteen systems, NCUA determined seven have high criticality for supporting agency operations. The CIO and OED plan to perform an annual review of systems and note any additions, disposals, or changes in criticality.

5. 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? Identify and describe the procedures for external reporting to law enforcement authorities and to the General Services Administration's Federal Computer Incident Response Center (FedCIRC). Identify actual performance according to the measures and the number of incidents reported in the format provided below. (Section 3534(b)(2)(F)(i)-(iii) of the Security Act.)

   A formal incident response capability has been documented, but is not yet implemented. NCUA needs to finalize the incident response policies and procedures and implement them. Because NCUA does not have an intrusion detection system, it is difficult for the agency to determine if there were any incidents or attempted breaches in security. NCUA has budgeted for and plans to deploy an intrusion detection system by the end of 2002.

a. Total number of agency components including bureaus, field activities.	*1*
b. Number of agency components with incident handling and response capability.	*1*

c. Number of agency components that report to FedCIRC.	*1*
d. Does the agency and its major components share incident information with FedCIRC in a timely manner consistent with FedCIRC and OMB guidance?	*NCUA did not report any incidents to FedCIRC during this reporting cycle.*
e. What is the required average time to report to the agency and FedCIRC following an incident?	*NCUA did not report any incidents to FedCIRC during this reporting cycle.*
f. How does the agency, including the programs within major components, confirm that patches have been tested and installed in a timely manner?	*Currently, the Information Security Officer has an informal process for overseeing the patch process. NCUA is in the process of implementing formal procedures that will identify and track the testing and installation of patches.*

	FY01	FY02
g. By agency and individual component, 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 by each component	*0*	*0*
h. By agency and individual component, number of incidents reported externally to FedCIRC or law enforcement.	*0*	*0*

C. Responsibilities of Agency Program Officials

1. Have agency program officials: 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? (Section 3534(a)(2) of the Security Act.)

   Most program officials have performed risk assessments using NIST 800-26 and developed security plans for each of the systems under their control. Of the nineteen systems identified at NCUA, eighteen of them

had security plans and risk assessments at the time of our review. However, program officials have not tested and evaluated controls of their respective systems.

NATIONAL CREDIT UNION ADMINISTRATION	TOTAL NUMBER OF SYSTEMS
TOTAL NUMBER OF AGENCY SYSTEMS	*19*

By each major agency component and aggregated into an agency total, from last year's report (FY01) and this reporting period (FY02) identify actual performance according to the measures and in the format provided below for the number and percentage of total systems.

NATIONAL CREDIT UNION ADMINISTRATION				
	FY01 #	FY01 %	FY02 #	FY02 %
a. Systems that have been assessed for risk.	*0*	*0%*	*18*	*95%*
b. Systems that have been assigned a level of risk after a risk assessment has been conducted (e.g., high, medium, or basic).	*0*	*0%*	*4*	*21%*
c. Systems that have an up-to-date security plan.	*0*	*0%*	*18*	*95%*
d. Systems that have been authorized for processing following certification and accreditation.	*0*	*0%*	*0*	*0%*
e. Systems that are operating without written authorization (including the absence of certification and accreditation).	*7*	*100%*	*1*	*5%*
f. Systems that have the costs of their security controls integrated into the life cycle of the system.	*0*	*0%*	*0*[1]	*0%*
g. Systems for which security controls have been tested and evaluated in the last year.	*1*	*14%*	*4*	*21%*
h. Systems that have a contingency plan.	*1*	*14%*	*2*	*11%*
i. Systems for which contingency plans that have been tested in past year.	*1*	*14%*	*1*	*5%*

[1] See D3.

2. For operations and assets under their control, have agency program officials used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency for their program and systems are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

   Other agencies or contractors maintain five systems used by NCUA. Program officials relied on external agencies and contractors to meet all applicable federal security requirements and assumed that their systems are secure. Program officials have not requested any evidence to support these assumptions, and therefore have not applied an appropriate level of due diligence to ensure these systems and services are adequately secure.

NATIONAL CREDIT UNION ADMINISTRATION		
	FY01	FY02
a. Number of contractor operations or facilities.	*5*	*5*
b. Number of contractor operations or facilities reviewed.	*0*	*0*

D. Responsibilities of Agency Chief Information Officers

1. Has the agency CIO: 1) adequately maintained an agency-wide security program; 2) ensured the effective implementation of the program and evaluated the performance of major agency components; and 3) ensured the training of agency employees with significant security responsibilities? Identify actual performance according to the measures and in the format provided below. (Section 3534(a)(3)-(5)) and (Section 3534(a)(3)(D), (a)(4), (b)(2)(C)(i)-(ii) of the Security Act.)

   The CIO developed and had oversight over the agency-wide security program and ensured effective implementation by working with program officials. The CIO and Security Officer assisted agency program officials with their risk assessments and security plans.

   During the course of the year, the Security Officer has attended security seminars that have enhanced the ability of the Security Officer to implement the agency wide security program. Other OCIO employees who are responsible for implementing technical security controls have attended various technical security seminars throughout the year. In August 2002, the Security Officer provided security awareness training to most employees at a bi-annual NCUA sponsored conference. However, new non-examiner employees and contractors with access to NCUA's

information technology resources did not receive any security training. The Security Officer's training at the conference was video taped and will be used for training new users of NCUA's information technology resources in the future.

		FY01	FY02
a.	Other than GAO or IG audits and reviews, how many agency components and field activities received security reviews?	*0*	*1*
b.	What percentage of components and field activities have had such reviews?	*0%*	*5%*
c.	Number of agency employees including contractors.	*1477*	*1451*
d.	Number and percentage of agency employees including contractors that received security training.	*7* *0%*	*1094* *75%*
e.	Number of employees with significant security responsibilities.	*7*	*16*
f.	Number of employees with significant security responsibilities that received specialized training.	*7* *100%*	*16* *100%*
g.	Briefly describe what types of security training were available.	*Technical seminars, conferences, and in-house training*	*Technical seminars, conferences, and in-house training*
h.	Total costs for providing training described in (g).	*$2,700*	*$1,500*

i.	Do agency POA&Ms account for all known agency security weaknesses including of all components and field activities? If no, why not?	*No, results from the CHRIS Audit, 2001 Financial Audit, and Penetration Test were not included in the POA&M.*
j.	Has the CIO appointed a senior agency information security official?	*Yes*

2. For operations and assets under their control (e.g., network operations), has the agency CIO used appropriate methods (e.g., audits or inspections) to ensure that contractor provided services (e.g., network or website operations) or services provided by another agency are adequately secure and meet the requirements of the Security Act, OMB policy and NIST guidance, national security policy, and agency policy? Identify actual performance according to the measures and in the format provided below. (Sections 3532(b)(2), 3533(b)(2), 3534(a)(1)(B) and (b)(1) of the Security Act.)

   NCUA utilizes agency employees to informally monitor contractors that supplement NCUA's information technology staff. In addition, a contractor maintains the backup storage facility. Program officials have assumed that the backup storage facility contractor met federal regulatory requirements and have not applied an appropriate level of due diligence to ensure that these services are adequately secure.

	FY01	FY02
a. Number of contractor operations or facilities.	*1*	*1*
b. Number of contractor operations or facilities reviewed.	*0*	*0*

3. Has the agency CIO fully integrated security into the agency's capital planning and investment control process? Were security requirements and costs reported on every FY03 capital asset plan (as well as in the exhibit 53) submitted by the agency to OMB? If no, why not? Identify actual performance according to the measures and in the format provided below. (Sections 3533(a)(1)(A)-(B), (b)(3)(C)-(D), (b)(6) and 3534(a)(C) of the Security Act.)

   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.

	FY03 Budget Materials	FY04 Budget Materials
a. Number of capital asset plans and justifications submitted to OMB?	*N/A*	*N/A*
b. Number of capital asset plans and justifications submitted to OMB without requisite security information and costs?	*N/A*	*N/A*
c. Were security costs reported for all agency systems on the agency's exhibit 53?	*N/A*	*N/A*
d. Have all discrepancies been corrected?	*N/A*	*N/A*
e. How many have the CIO/other appropriate official independently validated prior to submittal to OMB?	*N/A*	*N/A*

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL
OIG REPORT TO OMB ON NCUA COMPLIANCE WITH GOVERNMENT INFORMATION SECURITY REFORM ACT 2002

ATTACHMENTS

Exhibit 1:
Independent Evaluation of NCUA's Information Security Program Required by the Government Information Security Reform Act
- Executive Summary,
- Objectives, Scope, and Methodology,
- Consolidated Summary Report

Exhibit 2:
Financial Statement Audit 2001
- Executive Summary and Observations and Recommendations

Exhibit 3:
Evaluation of Project Risks Associated with Upgrade to Comprehensive Human Resources Integrated System
- Executive Summary

(Attachments transmitted separately.)