NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

OIG EVALUATION
GOVERNMENT INFORMATION
SECURITY REFORM ACT
2001

Report #OIG-01-09 **September 7, 2001**

Frank Thomas
Inspector General

Released by:
William A. DeSarno
Assistant Inspector General for Audits

William A. DeSarno

Auditor in Charge:
Tammy F. Rapp
Senior IT Auditor

Tammy F. Rapp, CPA

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL EVALUATION
GOVERNMENT INFORMATION SECURITY REFORM ACT
2001

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 Office of Management and Budget (OMB) has requested IGs to submit the results of their independent evaluation by responding specifically to questions 2 through 13 of OMB Memorandum M-01-24. The following presents our evaluation of the National Credit Union Administration's (NCUA) compliance with GISRA.

The NCUA Office of Inspector General (OIG) has determined that NCUA is not yet in compliance with GISRA. The following represents the agency's status toward compliance with key GISRA provisions as of August 2001:

- NCUA needs to develop an agency-wide security program. NCUA developed a draft security policy that will be incorporated in the security program. However this policy has not been approved by the agency head or disseminated to personnel with key responsibilities.
- NCUA needs to perform formal risk assessments.
- NCUA program managers need to perform periodic management testing of controls and perform their annual program review as required by GISRA.
- For the reporting cycle, NCUA has provided some security training to personnel with significant security responsibilities, and security awareness training is provided to all employees on a 3-year cycle coinciding with equipment replacement. New examiners are provided with basic computer training, which includes security awareness. Contractors and new non-examiner personnel are not provided any security awareness training.
- NCUA needs to formalize an incident response program.
- NCUA's Office of the Chief Information Officer (OCIO) needs to perform the annual security program review required by GISRA.
- NCUA has not yet determined the resources required to implement the security program and incorporate this program in the budget and strategic planning process.

Although we concluded that the agency is not in compliance with GISRA, we have not opined on actual security measures in place at the agency. According to the Chief Information Officer (CIO), NCUA has taken several steps to provide a secure environment, and as a result NCUA has not become aware of any significant security breaches. Some examples of proactive security practices include: matching risk to security controls; building controls into applications during development; and moving forward with new technologies that have increased security.

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL EVALUATION
GOVERNMENT INFORMATION SECURITY REFORM ACT
2001

The NCUA OIG with assistance from independent public accounting firms performed two audits during the reporting cycle that tested the effectiveness of information security and internal controls:

- On March 15, 2001, the OIG issued a report on our review of SAP Security & Control. SAP is used by NCUA to primarily perform online payment and accounting of agency financial transactions. The purpose of our review was to assess controls in the following areas: SAP Security; Data Integrity; Information Technology (IT) Infrastructure; and Business Processes. Our review included inquiry of personnel, observation of operations, and performance of tests within SAP. Our review identified several internal control weaknesses in the SAP security configuration. The most significant findings were related to segregation of duties and inappropriate user access privileges. NCUA's consolidated response to the 42 recommendations was positive, and NCUA stated all of the recommendations were either implemented or agreed to.

- On March 31, 2001, the OIG issued the Financial Statement Audit Report for the year ended December 31, 2000. The purpose of this audit was to express an opinion on whether the financial statements were fairly presented. In addition, the contractor reviewed the internal control structure and evaluated compliance with laws and regulations as part of the audit. The independent public accounting firm expressed unqualified opinions, stating that the financial statements were presented fairly. Although the independent public accounting firm did not find any matters considered to be material weaknesses in their review of the internal control structures pertinent to final reporting, they made six recommendations relating to weaknesses identified in the area of information security. NCUA agreed to implement all of the recommendations.

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL EVALUATION
GOVERNMENT INFORMATION SECURITY REFORM ACT
2001

OBJECTIVES, SCOPE, AND METHODOLOGY

OBJECTIVES:

The objectives of our review were to:

- Assess compliance with GISRA and agency security policies and procedures;
- Provide a synopsis of recent audits where tests of information security control techniques were performed for a subset of the agency's information systems; and
- Provide OMB with the results of our independent evaluation and specific evaluation of questions 2 through 13 of M-01-24.

SCOPE AND METHODOLOGY:

We reviewed the provisions of GISRA and associated OMB guidance. Our review procedures included inquiry of personnel with responsibilities associated with GISRA and some document review. We also reviewed the CIO's draft response to OMB's 01-24 dated August 31, 2001.

Our review focused on the agency's overall security framework, and we did not conclude on actual security measures in place.

This review was conducted at NCUA's Central Office in Alexandria, Virginia, during August 2001 and covered the period from January 2001 through August 2001.

NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL EVALUATION
GOVERNMENT INFORMATION SECURITY REFORM ACT
2001

OMB QUESTIONS 2 - 13

In specific response to OMB's Memorandum M-01-24, the OIG's evaluation of questions 2 through 13 is presented below:

2. *Identify the total number of programs included in the program reviews or independent evaluations.*

   NCUA has not identified programs for this purpose. However, NCUA identified seven mission critical systems. The agency should consider including other critical systems that are maintained by other agencies such as the agency's personnel processing system, payroll system, time and attendance system, disbursement system, etc. In addition, the agency needs to ensure that all critical systems have a program manager assigned with the responsibility for each system.

   The agency did not perform any program reviews during this reporting cycle. The OIG performed two independent evaluations that included information security and internal controls during this 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.

3. *Describe the methodology used in the program reviews and the methodology used in the independent evaluations.*

   a. SAP Security Review

      The overall objective of the SAP Security Review was to ensure that the existing control environment and security infrastructure of the SAP system was adequate. The review included assessment of controls in the areas of SAP security, data integrity, information technology infrastructure, and business processes surrounding the SAP modules. Review procedures included inquiry of personnel, observation of operations, and performance of tests within SAP.

   b. 2000 Financial Statement Audits

      The purpose of the financial statement audits was to express an opinion on whether the financial statements were fairly presented. In addition, the internal control structure and compliance with laws and regulations were evaluated. The audit procedures included inquiry of personnel, review of policies and procedures, observation of operations, and limited testing of information technology controls.

4. *Report any material weakness in policies, procedures, or practices as identified and required to be reported under existing law.*

   Although no material weaknesses were reported under existing law, our review of the financial system revealed many significant security weaknesses. According to agency officials, these weaknesses have been addressed. As a result of this evaluation, we observed material weaknesses and made several recommendations regarding the agency's

overall information security framework. The OIG plans to perform a follow-up review of all security related recommendations during the next reporting cycle.

5. *Describe the specific measures of performance used by the agency to ensure that agency program officials have: 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. Include information on the actual performance for each of the four categories.*

    a. Although the annual appraisal process is a tool used by the Office of the Executive Director (OED) to ensure managers fulfill their responsibilities, there were no specific measures of performance to ensure that agency program officials have performed the following:
        - Assessed the risk to operations and assets under their control;
        - Determined the level of security appropriate to protect such operations and assets;
        - Maintained an up-to date security plan for each system supporting the operations and assets under their control; and
        - Periodically tested and evaluated security controls and techniques.

    b. NCUA program officials:
        - Have not performed any formal risk assessments for operations and assets under their control;
        - Although it appears that program officials participate in determining some level of security and controls over their respective operations, this process is informal and undocumented. The OIG was unable to determine if their determination of controls was based on an evaluation of the risks to information systems and data and the costs of implementing specific controls;
        - Have not developed a security plan for each system supporting the operations and assets under their control; and
        - Have not periodically tested and evaluated security controls and techniques for systems under their control.

6. *Describe the specific measures of performance used by the agency to ensure that the agency CIO: 1) adequately maintains an agency-wide security program; 2) ensures the effective implementation of the program and evaluates the performance of major agency components; and 3) ensures the training of agency employees with significant security responsibilities. Include information on the actual performance for each of the three categories.*

    a. Although the annual appraisal process is a tool used by OED to ensure managers fulfill their responsibilities, there were no specific measures of performance to ensure that the agency CIO:
        - Adequately maintains an agency-wide security program;
        -

- Ensures the effective implementation of the program and evaluates the performance of major agency components; and
- Ensures the training of agency employees with significant security responsibilities.

b. The CIO:

- Recently assigned the role of senior information security official to a senior information technology specialist as part of his ancillary responsibilities;
- Has not developed an agency-wide security program or ensured the effective implementation of the program and evaluated the performance of major agency components;
- Has ensured the training of agency employees with significant security responsibilities.

7. *Describe how the agency ensures that employees are sufficiently trained in their security responsibilities. Identify the total number of agency employees and briefly describe what types of security training was available during the reporting period, the number of agency employees that received each type of training, and the total costs of providing such training.*

   NCUA provided security training to all employees in conjunction with its notebook computer replacement in Spring 2000. New examiners are provided with basic security training when they are provided with their equipment. However, new non-examiner employees and contractors with access to NCUA's information technology resources do not receive any security training. NCUA should consider providing periodic security awareness updates to all employees and contractors.

8. *Describe the agency's documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. Include a description of procedures for external reporting to law enforcement authorities and to the General Services Administration's Fed CIRC. Include information on the actual performance and the number of incidents reported.*

   NCUA does not have documented procedures for reporting security incidents and sharing information regarding common vulnerabilities. NCUA's security incident process is informal and undocumented.

9. *Describe how the agency integrates security into its capital planning and investment control process. Were security requirements and costs reported on every FY02 capital asset plan (as well as exhibit 53) submitted by the agency to OMB? If no, why not?*

   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. NCUA has not taken any steps to ensure that plans to fund and manage security are built into life-cycle budgets for information systems.

10. Describe the specific methodology used by the agency to identify, prioritize, and protect critical assets within its enterprise architecture, including links with key external systems. Describe how the methodology has been implemented.

NCUA plans to complete its enterprise architecture by June 30, 2002.

11. Describe the measures of performance used by the head of the agency to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system. Include information on the actual performance.

a. Specific measures of performance have not been identified to ensure that the agency's information security plan is practiced throughout the life cycle of each agency system.

b. NCUA informally incorporated information security throughout the life cycle of each agency system.

12. Describe how the agency has integrated its information and information technology security program with its critical infrastructure protection responsibilities, and other security programs (e.g., physical and operational).

NCUA intends to integrate all of its security responsibilities when it develops the agency-wide information technology security program.

13. Describe the specific methods (e.g., audits or inspections) used by the agency 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.

a. NCUA utilizes agency employees to informally monitor contractors that supplement NCUA's information technology staff.

b. NCUA has not performed any steps to ensure that 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.

RECOMMENDATIONS

In order to comply with GISRA:

1. The Executive Director should develop specific performance measures to ensure that a successful security program is developed, maintained, and implemented throughout the agency.

2. The Executive Director should develop specific performance measures to ensure that senior program managers have:
    a. Assessed the risk to operations and assets under their control;
    b. Determined the level of security appropriate to protect such operations and assets;
    c. Maintained an up-to-date security plan for each system supporting the operations and assets under their control; and
    d. Periodically tested and evaluated security controls and techniques.

3. The Executive Director should develop specific performance measures to ensure that the CIO:
    a. Adequately maintains an agency-wide security program;
    b. Ensures the effective implementation of the program and evaluates the performance of major agency components; and
    c. Ensures the training of agency employees with significant security responsibilities.

4. The Executive Director should ensure that the agency has trained all personnel sufficient to assist the agency in complying with the requirements of GISRA and related agency security policies and procedures.

5. The Executive Director should develop specific performance measures to ensure that the CIO and senior program managers:
    a. Annually evaluate the effectiveness of the agency information security program, including testing control techniques, and implement appropriate remedial actions based on the evaluation; and
    b. Report the results of such tests and evaluations and progress made on remedial actions.

6. The Executive Director should evaluate the resources required to implement the security program and consider such resources in the annual budgeting and strategic planning process.

7. The Executive Director should ensure that security is incorporated with its strategic plan and enterprise architecture.

8. The CIO should develop and maintain an agency-wide security program that integrates all of NCUA's security responsibilities and includes the following elements:

a. Periodic risk assessments that consider internal and external threats to the integrity, confidentiality, and availability of systems and data;
b. Policies and procedures that are based on risk assessments that cost effectively reduce information security risks to an acceptable level;
c. Periodic security awareness training to inform and remind all employees, contractors, and other users of agency systems of their information security risks and respective security responsibilities;
d. Periodic management testing and evaluation of the effectiveness of information security policies and procedures;
e. A process for ensuring remedial action to address any significant deficiencies; and
f. Procedures for detecting, reporting, and responding to security incidents.

9. The CIO should ensure that the agency effectively implements and maintains information security policies, procedures, and control techniques.

10. The CIO should propose through the agency budget process that the senior information security official is given adequate resources to perform security related responsibilities.

11. The CIO should perform an annual evaluation of the agency-wide security program.

12. The CIO should develop specific methods to ensure the adequate security of contractor provided services.

13. Senior program managers should assess the information security risks associated with the operations and assets for programs and systems over which they have control. These risk assessments should be documented and periodically reevaluated.

14. Senior program managers should determine the levels of information security appropriate to protect operations and assets under their control. These control assessments should be documented and periodically reevaluated.

15. Senior program managers should periodically test and evaluate information security controls and techniques, as well as perform an annual program review in consultation with the CIO.

16. Senior program managers should develop a security plan for each system supporting the operations and assets under their control.

17. Senior program managers should develop specific methods to ensure that information technology services provided by other agencies are adequately secure.

18. The CIO should assist the senior program managers with their responsibilities outlined above.

The initial response we received from the Office of the Executive Director indicated they generally agreed with all of the above recommendations.

ATTACHMENTS

Exhibit 1: SAP Security Audit
(Executive Summary)
Exhibit 2: Financial Statement Audit 2000
(Executive Summary and Observations and Recommendations)

(Attachments transmitted separately.)