NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

INDEPENDENT EVALUATION OF NCUA'S INFORMATION SECURITY PROGRAM REQUIRED BY GOVERNMENT INFORMATION SECURITY REFORM ACT 2002

Report #OIG-02-11 **September 30, 2002**

Acting Inspector General:

William A. DeSarno

Auditor in Charge:

Tammy F. Rapp, CPA

NATIONAL CREDIT UNION ADMINISTRATION - OFFICE OF INSPECTOR GENERAL INDEPENDENT EVALUATION OF NCUA'S INFORMATION SECURITY PROGRAM - 2002

Executive Summary

The Government Information Security Reform Act (GISRA) is part of the Defense Authorization Act (Public Law 106-398, Title X, Subtitle G). The law requires each Federal agency to develop, implement and review a comprehensive agency-wide security program. The Act pertains to all systems supporting all operations of the agency including those systems currently in place or planned. For some agencies, the Act also extends to contractor systems if they are used by the agency to support operations. The agency head is required to submit an annual report to Congress summarizing the findings/issues found during the year. To accomplish these requirements, the Act requires that agencies perform independent internal reviews and security testing.

Key GISRA requirements include:

- An annual independent evaluation of agency information systems security controls.
- An examination of the adequacy and effectiveness of information security policies, procedures and practices.
- An assessment of compliance with the requirements of the Act.
- An annual report submitted to Congress by the agency head summarizing the findings/issues found during the year.

The information technology infrastructure supporting NCUA's nineteen mission critical systems is composed of a wide-area network with servers, notebooks and desktop computers. This infrastructure provides the computing platform for all major business applications of NCUA. The platform includes all IT hardware, communications, network storage, central databases and operating systems. Servers are configured with either Microsoft NT or Microsoft Windows 2000 operating systems, and provide a variety of services.

According to NCUA's GISRA 2001 Report, we determined that NCUA was not yet in compliance with GISRA. The following represented the agency's status toward compliance with key GISRA provisions as of August 2001:

- NCUA needed to develop an agency-wide security program. NCUA developed a draft security policy that would be incorporated in the security program. However this policy was not approved by the agency head or disseminated to personnel with key responsibilities.
- NCUA needed to perform risk assessments.
- NCUA program managers needed to perform periodic management testing of controls and perform their annual program review as required by GISRA.

- For the reporting cycle, NCUA had provided some security training to personnel with significant security responsibilities, and security awareness training was provided to all employees on a 3-year cycle coinciding with equipment replacement. New examiners were provided with basic computer training, which included security awareness. Contractors and new non-examiner personnel were not provided any security awareness training.
- NCUA needed to formalize an incident response program.
- NCUA's Office of the Chief Information Officer (OCIO) needed to perform the annual security program review required by GISRA.
- NCUA had not yet determined the resources required to implement the security program and incorporate this program in the budget and strategic planning process.

During the past year, NCUA prepared an overall agency security plan in addition to security plans for each mission critical system. NCUA also performed risk assessments for each mission critical system using the National Institute of Standards and Technology (NIST) Special Publication 800-26, "Security Self-Assessment Guide for Information Technology Systems."

During 2002, the Office of Inspector General (OIG) contracted with Urbach Kahn & Werlin, LLP SACteam™, Information Risk Management Services Group (UKW), to evaluate the agency- wide plan, as well as each individual system security plan and risk assessment in depth. In addition, implementation of prior security related audit recommendations and the agency's plans of action and milestones were evaluated. Establishing and maintaining effective security controls are important responsibilities of the management of the system owners and the agency. Effective security controls are essential to achieving the requirements of GISRA. The primary objective of this review was to assess that controls that are required to be established as provided by GISRA and prior promulgation (OMB A-130 Appendix III, Computer Security Act of 1987, Clinger-Cohen Act of 1996, the Paperwork Reduction Act of 1995, et al.) are in place and operating as designed.

Summary Conclusion

The NCUA OIG determined that NCUA is actively working towards compliance with GISRA. Risk assessments and security plans were completed for all but one of NCUA's mission critical systems. Specifically, a risk assessment and corresponding security plan was not completed for: the General Service Administration (GSA)'s Payroll, Accounting and Reporting System (PAR). Subsequent to our review, NCUA contacted GSA and performed a risk assessment and prepared a security plan for PAR. In addition, we noted and detailed conditions of risk and made recommendations for improvement relevant to each of the applications reviewed. These are detailed in the individual report section and, are being addressed by the program officials and Office of the Chief Information Officer (OCIO) as required. Each of the items listed in these reports have been discussed with, reviewed and concurred by the respective program officials and the Information Security Officer. NCUA management comments are summarized at the end of each individual report section. None of the individual application risk conditions affect the overall recommendation regarding GISRA compliance detailed in the subsequent paragraph.

The OIG supports reporting NCUA's GISRA compliance at Level 2 (see page 60). The majority of the critical elements under review are rated at Level 2 (e.g., policies and procedures are in draft format) or Level 3 (e.g., the relevant policies and procedures are approved and implemented). A Level 2 or 3 rating is applied to each of the systems except for PAR, which was discussed in the preceding paragraph. We have applied a Level 0 rating for all of the systems regarding the certification/re-certification and authorization to process within NCUA's information system architecture.

The remainder of this report is restricted for Limited Official Use only.