Appendix A

# NATIONAL CREDIT UNION ADMINISTRATION
# OFFICE OF INSPECTOR GENERAL

## INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION INFORMATION SECURITY PROGRAM 2006

**Report #OIG-06-05** **September 29, 2006**

William A. DeSarno

*William A. DeSarno*
*Inspector General*

*Released by:*

*James Hagen*
*Asst IG for Audits*

*Auditor-in-Charge:*

Tammy F Rapp

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

## CONTENTS

# I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged Grant Thornton LLP to conduct an independent evaluation of its information systems and security program and controls for compliance with the Federal Information Security Management Act (FISMA), Title III of the E-Government Act of 2002.

Grant Thornton evaluated NCUA's security program through interviews, documentation reviews, and sample testing. We evaluated NCUA against standards and requirements for federal government agencies such as those provided through FISMA, National Institute of Standards and Technology (NIST) Special Publications (SPs) and Federal Information Processing Standards (FIPS), and Office of Management and Budget (OMB) memorandums. We conducted an exit conference with NCUA officials on September 6, 2006, to discuss evaluation results.

The NCUA made noticeable progress in strengthening its Information Technology (IT) security program during Fiscal Year (FY) 2006. Notable accomplishments include:

- Significant strides in remediation of the significant deficiency noted in the FY2005 report by deploying encryption software to improve security of information stored on examiners' laptop computers, and
- Completion of the Accreditation package for the NCUA General Support System (GSS).

While NCUA has made commendable progress in eliminating the significant deficiencies reported last year, our review this year identified the following weaknesses in IT security controls that deserve immediate management attention:

- Procedures requiring the use of cryptographic security measures for sensitive financial and Personally Identifiable Information (PII) need better enforcement, and Privacy Impact Assessments (PIA) for its systems needs to be developed.

- Certification and accreditation (C&A) of all NCUA systems needs to be completed.

- Password and user account security configurations need improvement, including regular user account reconciliations.

- Personnel security awareness training program needs to be fully implemented.

We also noted the following other weaknesses in IT security controls that management should consider:

- Security planning documentation needs improvement in consistent version control, revisions/updates, and dissemination to required officials.

- E-Authentication risk assessments should be developed for NCUA's systems.

- Security configuration guides need to be developed.

- Continuity of Operations Plan (COOP) and Disaster Recovery procedures need to be more consistently updated and tested including the regular testing of NCUA's Disaster

Recovery and system contingency plans. In addition, restoration priorities related to system impact ratings need to be consistently applied and documented.

- Physical security measures need to be consistently enforced.
- Regular incident response training needs to be conducted.
- NCUA's Plan of Actions and Milestones (POA&M) process needs improvement.

We appreciate the courtesies and cooperation provided to our auditors during this audit.

.

# II. BACKGROUND

This section provides background information on FISMA and NCUA.

## FEDERAL INFORMATION SECURITY MANAGEMENT ACT

The President signed into law the E-Government Act (Public Law 107-347), which includes Title III, Information Security, on December 17, 2002. FISMA permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues annual review and reporting requirements introduced in GISRA. In addition, it includes new provisions aimed at further strengthening the security of the federal government's information and information systems, such as development of minimum standards for agency systems. In general, FISMA:

- Lays out a framework for annual information technology security reviews, reporting, and remediation plans.
- Codifies existing OMB security policies, including those specified in Circular A-130, *Management of Federal Information Resources*, and Appendix III.
- Reiterates security responsibilities outlined in the Computer Security Act of 1987, Paperwork Reduction Act of 1995, and Clinger-Cohen Act of 1996.
- Tasks NIST with defining required security standards and controls for federal information systems.

OMB issued the 2006 Reporting Instructions for the Federal Information Security Management Act on July 17, 2006. This document provides clarification to agencies for implementing, meeting, and reporting FISMA requirements to OMB and Congress.

## NATIONAL CREDIT UNION ADMINISTRATION

NCUA is the independent federal agency that charters, supervises, and insures the nation's federal credit unions, and it insures many state-chartered credit unions as well. NCUA is funded by the credit unions it supervises and insures. NCUA's mission is to foster the safety and soundness of federally-insured credit unions and to better enable the credit union community to extend credit for productive and provident purposes to all Americans, particularly those of modest means.

NCUA strives to ensure that credit unions are empowered to make necessary business decisions to serve the diverse needs of its members and potential members. It does this by establishing a regulatory environment that encourages innovation, flexibility, and a continued focus on attracting new members and improving service to existing members.

NCUA has a full-time three-member board appointed by the President of the United States and confirmed by the Senate. The Board consists of a chairman, vice chairman, and member. No more than 2 board members can be from the same political party, and each member serves a staggered 6-year term. NCUA's board regularly meets in open session each month with the exception of August, in Alexandria, Virginia. In addition to its central office in Alexandria, NCUA has five regional offices and the Asset Management and Assistance Center (AMAC).

## III. OBJECTIVE

The engagement objective was to assist the OIG in performing an independent evaluation of NCUA information security policies and procedures for compliance with FISMA and federal regulations and standards and to evaluate the following efforts:

- Efficiency and effectiveness of the agency's information security program
- Agency's progress in meeting responsibilities under FISMA
- Agency's progress in remediation of prior audit weaknesses relating to FISMA and other security weaknesses identified
- Agency progress in implementing its plans of action and milestones (POA&M)

Additionally, the audit was required to provide sufficient supporting evidence of NCUA's security program evaluation to enable the OIG to report to OMB.

## IV. METHODOLOGY AND SCOPE

Our evaluation compared NCUA's information security program and practices with FISMA and federal criteria contained in the Government Accountability Office's *Federal Information System Controls Audit Manual (FISCAM)*, as well as other relevant guidance from NIST and OMB.

We conducted a review of information security control techniques for all of NCUA's major information systems on a rotational basis. During this evaluation, we completed assessment of NCUA controls over access controls, incident management and reporting, and additional areas required to report under OMB M-06-20. This included reviews of C&A documentation such as system security plans, risk assessments, contingency plans, and certification reports. In addition, we reviewed existing information security controls and identified weaknesses impacting certain components affecting GSS security.

We did not conduct penetration testing during this evaluation. Our testing efforts, scheduled on a rotational basis, will conduct penetration testing during a future evaluation.

We performed our engagement in accordance with generally accepted government auditing standards (GAGAS), audit standards promulgated by American Institute of Certified Public Accountants (AICPA), and information systems standards issued by the Information Systems Audit & Control Association (ISACA).

# V. RESULTS IN DETAIL

Security program planning and management controls are designed to provide the framework and continuing cycle of activity for managing risk, developing security policies, assigning responsibilities, and monitoring the adequacy of an entity's computer-related controls. We identified weaknesses that require management's attention, and they are discussed below.

## 1. NCUA should do more to enforce procedures requiring the use of cryptographic security measures in protecting sensitive financial and Personally Identifiable Information.

Current security procedures should be improved to better enforce the use of cryptographic security measures in securing sensitive financial and Personally Identifiable Information (PII) used by credit union examiners to conduct their audits. We noted several areas where improvement is needed in enforcing the use of encryption for exam data below:

- Laptop encryption: While all AIRES files contain information considered both sensitive and PII related to financial disclosure, not all AIRES files are encrypted on examiner laptops. In all of the examiner laptops examined, exam files, produced by AIRES and containing sensitive personal and financial information, were stored outside the encrypted directory and available in plaintext.

- Encryption of Data at Rest: Examiners are issued external hard drives for use in periodic (weekly) backups. We examined one external hard drive and found that it did not utilize any encryption technology for most of the data at rest. The pervasiveness of this practice was confirmed by the NCUA Information Security Officer (ISO). Additionally, these drives are stored at the examiners home offices.

- Deletion of sensitive files: The examiners interviewed noted they do not immediately delete sensitive files that are for credit union examinations they have completed. When examiners do delete files, they simply hit the “delete” key. This means copies of deleted files likely reside in the recycle bin and are not overwritten in order to prevent restoration. In addition, we observed hundreds of old files that were maintained on an examiner’s drive that were not needed.

- Multiple, non-encrypted media storage: Examiners use various media for backup and sharing purposes in between weekly backups to their external drive. The examiners confirmed the use of CDs and/or personal USB drives at a minimum. We observed files containing sensitive and PII data on these media that were not encrypted. Due to the size and portability of this type of media, NCUA is at great risk of losing or misplacing this media with sensitive personal and financial data.

By not implementing procedures to ensure the selected process for encryption of sensitive data is utilized, regardless of the storage media, NCUA potentially increases the risk of inadvertent disclosure of sensitive information which, in turn, increases the risk to NCUA data confidentiality and integrity, as well as potential identity theft of credit union members.

The Federal Information Security Management Act provides guidance related to these conditions:

> *Provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of agency information. (Section 301, 3544, a1,A)*

**Recommendation:** We recommend that NCUA management enforce the encryption of all sensitive data on all laptops, portable devices, and storage media. Additionally, user training should be enhanced to specifically address the need for securing and encrypting sensitive data (including that beyond Social Security Numbers).

***Agency Response:*** Agreed. As you know, we have made substantial progress and will continue to improve.

We have;

- Encrypted sensitive data on most of the laptops, thumb drives and external hard drives,
- Conducted training on this subject at the regional conferences.

We will;

- Force encryption on the laptops and external hard drives that have not yet been done manually,
- Modify the rules of behavior to further bring awareness to this subject.

**OIG Response:** *The OIG concurs.*

### 2. Privacy Impact Assessments (PIA) are needed for NCUA systems.

The NCUA has not completed a privacy impact assessment for its data or systems. While certification and accreditation activities have been completed or are in process, a formal consideration of privacy has not occurred. The NCUA has asserted that the requirement to complete a PIA does not apply to the agency and therefore has not been completed. Completion of the PIA was noted as being required during the previous year's FISMA evaluation as part of C&A requirements. The NCUA increases the risk of sensitive information being inadvertently disclosed to unauthorized persons and the potential impact to personally identifiable information is not assessed.

The E-Government Act guides agencies to:

> *To conduct a PIA before: developing or procuring IT systems or projects that collect, maintain or disseminate information in identifiable form from or about members of the public or initiating, consistent with the Paperwork Reduction Act, a new electronic collection of information in identifiable form for 10 or more persons (excluding agencies, instrumentalities or employees of the federal government). In general, PIAs are required to be performed and updated as necessary where a system change creates new privacy risk.*

**Recommendation:** We recommend that NCUA management complete a privacy impact assessment over its data.

***Agency Response:*** While management believes a privacy review of all "data" is a commendable goal, management maintains its position that a PIA, as contemplated by the E-Government Act, is not required.

Management acknowledges that the agency is subject to the requirement to prepare PIAs as provided in the E-Government Act. Management's view is that the requirement to prepare a PIA, required under the E-Government Act that became effective April 17, 2003, is triggered where an agency develops or procures an IT system or changes an existing system by adding new uses or new technologies or significantly changes how information in identifiable form is managed in the system. Generally, a PIA is required where a system change creates new privacy risks. *See* OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002 (M-03-22).

NCUA last updated its Systems of Records notice effective in February 2000. *See* 65 Fed. Reg. 3486 (Jan. 21, 2000). Management's position is that, with the exception of the new Personnel Security and Identity Management Systems required under the Homeland Security Presidential Directive-12 (HSPD-12), the agency has neither developed nor procured new IT systems nor made a significant change to an existing system that created new privacy risks requiring preparation of a PIA. At this time, the agency is in the process of developing a PIA for these new systems, updating its Systems of Records notice, and preparing related notices and instructions for employees.

Management maintains its view that it is not required to prepare and publish a PIA conforming to the requirements of the E-Government Act for IT systems in existence before April 2003 and which have been maintained without significant change. It is our position that our ongoing maintenance of these systems has not had an impact on the *privacy risk* of those systems. Routine maintenance does not change the basic functions of the programs; it normally entails updates to the user interface, revised edit formulas, etc., which have no bearing on the privacy risk level. Nevertheless, management acknowledges that a review of existing IT systems to ensure compliance with information privacy laws, regulation, and policy is an appropriate and commendable agency aspiration and intends to undertake such review as agency resources permit.

**OIG Response:** *Per the requirements of section 208 of the E-Government Act of 2002, OMB issued guidance to agencies regarding the development of PIAs. The guidance provided by OMB applies to all executive branch departments and agencies. The Act requires agencies to conduct a PIA before developing or procuring IT systems that collect, maintain, or disseminate information in identifiable form from or about member of the public as well when the changes occur in information collection authorities, business processes or other factors affecting the collection and handling of such information. Since the inception of the E-Gov Act, NCUA has implemented several changes to business process and technical solutions that meet the above criteria as changes requiring an update or development of a PIA, including the distribution of external hard drives to store credit union audit data that are stored at the examiners' homes, an agency-wide update in operating systems (from 2000 to XP), distribution of new laptops, and partial implementation of sensitive data encryption.*

*It is the opinion of the OIG that any one of the above changes constitutes a change of the magnitude that requires the development of a PIA. Based on the identified changes to the methods of collecting, processing, and storing personally identifiable information with the agency's IT infrastructure, NCUA should develop a PIA and maintain it on an ongoing basis.*

### 3. Certification and accreditation (C&A) activities have not been completed for all NCUA systems.

The NCUA continues to conduct ongoing certification and accreditation activities for its systems. A standard protocol has been developed, incorporating NIST SP 800-53 control baselines, and used to conduct certification tests on all major NCUA systems. An outside vendor was contracted during 2005 to assist the NCUA in certifying and accrediting the GSS and NAS systems. As a result of this process, the GSS has been fully certified and accredited. The NAS, ESS, CRS, and IIS systems are currently undergoing certification and accreditation activities and were not complete as of the end of our field work.

In addition to not completing the certification and accreditation of all NCUA systems, our evaluation of the overall C&A process identified the following weaknesses:

- While the GSS has been fully certified and accredited, its system security plan (SSP) needs to be updated to reflect the current NCUA environment. The current NCUA documentation does not reflect a consistent, accurate overview of the GSS technical environment as it currently exists. Notable exceptions include:

  - Continued reference to ZoneAlarm™ personal firewalls, which have been removed.
  - No accounting for minor applications as they relate to the overall risk of the GSS infrastructure.
  - Technology such as Voice over Internet Protocol (VoIP) which requires additional security considerations (see NIST 800-58) are not addressed.
  - The version of the GSS SSP provided does not reflect version control (i.e. record changes) or dissemination instructions.

  The lack of adequately documented security requirements in the GSS SSP may impact NCUA's ability to continuously and comprehensively monitor overall risk and maintain security configuration commensurate with that risk.

- The NCUA security documentation does not support consistent application of impact assessment rankings in accordance with FIPS 199. Our evaluation noted instances of systems having different FIPS 199 impact rankings between the risk assessment and system security plan.

  By not using a standardized approach to assessing FIPS 199 impact rankings, NCUA potentially limits the ability to apply required security controls commensurate to systemic risk to confidentiality, integrity, and availability.

- The NCUA has not fully documented Interconnection Security Agreements (ISA), Memorandums of Understanding (MOU), or Memorandums of Agreement (MOA) for all of its systems connections to outside agencies. While connections to the Federal Reserve and GSA have been documented, connections to the Department of Treasury and to Pay.Gov have not.

  By not formally documenting system interconnections with other agencies/organizations, NCUA increases the risk of connecting to a system that does not meet the security requirements of its own system. Thus increasing the risk to NCUA's data confidentiality, integrity, and availability

OMB Circular A-130, Appendix III, *Security of Federal Automated Information Resources*, provides the following guidance related to these conditions:

> *Ensure that a management official authorizes in writing the use of each general support system based on implementation of its security plan before beginning or significantly changing processing in the system. Use of the system shall be re-authorized at least every three years (Section A.3.a.4).*

FIPS 199 guides agencies in assigning security categorizations and requires:

> *Agencies to assign security categories that are based on the potential impact on an organization should certain events occur which jeopardize the information and information systems needed by the organization to accomplish its assigned mission, protect its assets, fulfill its legal responsibilities, maintain its day-to-day functions, and protect individuals (i.e. Privacy Act or PII).*

NIST SP 800-18, *Guide for Developing Security Plans for Federal Information Systems*, provides additional guidance relating to the development of system security plans:

> *An ISA, MOU, or MOA is needed between systems (not between workstations/desktops or publicly accessed systems) that share data that are owned or operated by different organizations. (Section 3.1.1)*
>
> *Additionally, it guides that the Information System Owner must update the system security plan whenever a significant change occurs. (Section 1.7.2)*

**Recommendation:** We recommend that NCUA management: complete its C&A activities for the NAS, ESS, CRS and IIS systems; periodically review and update the SSPs as part of configuration and risk management; and ensure that security categorizations are completed in accordance with FIPS guidance. Additionally, we recommend that NCUA management formally document all of its system interconnections with outside agencies and/or organizations through the use of the MOU, ISA, or MOA.

***Agency Response:*** Agreed. We are continuing to complete the certification processes and have already completed the FIPS categorization.

**OIG Response:** *The OIG concurs.*

### 4. Regular user account reconciliations are not conducted to ensure that only user accounts with a business purpose exist.

The NCUA does not conduct regular user account reconciliations over its account population, which has resulted in an excessive number of system and temporary accounts on the system. Additionally, after further discussion, we noted that NCUA has not implemented a temporary account policy or procedure.

The NCUA, based on our discussions surrounding this matter, have recently completed a reconciliation that is to identify potentially unneeded system and temporary accounts and address them. Additionally, a third-party product is being implemented to automate the user account review process.

Additionally, as a result of not conducting formal user account reconciliations, we identified an instance of a separated employee not being timely removed from NCUA systems. Documentation illustrating the request for removal of a user account did not occur timely for one NCUA separated employee. The employee did not have an exit email documented. A follow up email dated June 02, 2006 was sent to verify that he could be removed from the NCUA system. He separated from NCUA on February 2, 2006. Also, the follow up email notes that his last logon was March 8, 2006 which is after his separation date.

By not conducting regular user account reconciliations, NCUA increases the risk of having outdated accounts active on the system which may elevate the opportunity for an unauthorized person to gain access to NCUA systems.

NIST Special Publication 800-53 provides guidance for these conditions:

> *The organization must manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts. The organization must review information system accounts.*

OMB Circular A-130, Appendix III also guides that agencies establish controls to assure adequate security for all information processed, transmitted, or stored in Federal automated information systems.

**Recommendation:** We recommend that NCUA management establish system and temporary user account policy and procedures and implement a regular user account reconciliation process. Additionally, we recommend that NCUA consistently follow its employee enter, exit, or change procedures and send a notice to all offices reminding them of this policy.

***Agency Response:*** Agreed.

**OIG Response:** *The OIG concurs.*

### 5. NCUA password and user account security configurations need improvement.

During our evaluation we noted several instances of NCUA password and user account security configurations that need improvement. In general, NCUA network password settings apply only to network applications and resources, not to end-user laptops and desktops. Therefore, a user could enter an unlimited number of invalid passwords, but would only be restricted from using network applications like email if the password attempt threshold is exceeded. According to the NCUA ISO, this practice is in place because remote users would need to physically ship their laptop to the Central Office facility to have their password reset in the event of a lockout.

Additionally, we noted other conditions relating to NCUA's password and user account security configuration below:

- NCUA password policy allows the same password to be used for too long a period of time by not currently forcing users to change their passwords.

- After exceeding the allowed number of failed login attempts, users are only restricted from accessing network resources, not from the laptops themselves.
- NCUA applications do not log users out following a limited period of inactivity and password protected screensavers for Central Office personnel engage after too long a period of user activity.

Allowing users to maintain the same password indefinitely greatly increases the chance of the user's password being discovered. Also, by allowing an infinite number of invalid login attempts, an unauthorized individual with access to a laptop could attempt as many passwords as necessary until they guessed the correct password. Additionally, by tolerating extended periods of inactivity, NCUA potentially increases the risk of unauthorized access to sensitive resources.

NIST SP 800-53 provides guidance to agencies on these conditions. It guides that:

> *For password-based authentication, the information system enforces password minimum and maximum lifetime restrictions. (Section IA-5)*
>
> *The information system prevent further access to the system by initiating a session lock that remains in effect until the user reestablishes access using appropriate identification and authentication procedures. The information system also activates session lock mechanisms automatically after a specified period of inactivity defined by the organization. (Section AC-11)*
>
> *The information system enforces a limited number of consecutive invalid access attempts by a user during an organization-defined time period. The information system should automatically lock the account or delay next login prompt when the maximum number of unsuccessful attempts is exceeded. (Section AC-7)*

**Recommendation:** We recommend that NCUA management:

- Require users to change their password every 90 days.
- Fully lock user accounts, including laptops and desktops, after the maximum number of failed login attempts has been made.
- Password protect network applications and computers after 30 minutes of inactivity.

***Agency Response:***

- Agree with the first bullet.
- We evaluated this and concluded that it is not in the best interest of the agency due to the remote nature of most of our users.
- OMB M-06-16 states that all mobile computers must be set to lock-out after 30 minutes. We have determined that this is an appropriate practice. The time-out is now set to 30 minutes for all laptops.

**OIG Response**: *The OIG concurs with the agency's response referring to the lock-out and has changed the recommendation to 30 minutes. However, the choice not to limit failed user attempts should be documented and compensating controls identified.*

### 6. The NCUA personnel security awareness program has not been fully implemented.

The NCUA personnel security awareness training program has not been fully implemented. To accomplish security awareness training, the NCUA relies on the Rules of Behavior document that describes NCUA's information security policies and requires that NCUA employees acknowledge their understanding of them. However, not all NCUA employees and contractors have signed the NCUA Rules of Behavior document noting their understanding and agreement to the NCUA security policies. In addition, SSAs have not been provided with NCUA Rules of Behavior or similar agreement. Additionally, not all NCUA personnel with significant security responsibilities have received additional security training.

The NCUA security awareness program is in the process of being completed. As of the time of this finding, not all NCUA employees have signed the NCUA Rules of Behavior document noting their understanding and agreement to the NCUA security policies. By not having all employees complete security awareness training, NCUA increases the risk of employees conducting their duties in a manner that is not in compliance with NCUA policy and may increase the risk to NCUA data confidentiality, integrity, and availability.

NCUA Agency Wide Information Security Policy, section 3.1.3 requires:

> *Training oversight has two parts, general awareness training and specific training for people with significant security responsibilities. The CIO will review the reports specified in section 3.2.3 to ensure adequate training is planned for NCUA.*

NIST SP 800-53 guides that:

> *The organization ensures system managers, system administrators, and other personnel having access to system-level software have adequate technical training to perform their assigned duties. (Section AT-3)*

**Recommendation:** We recommend that NCUA management complete their process of fully implementing their security awareness training program and ensure that all employees, contractors, and SSAs who have access to NCUA data sign the NCUA Rules of Behavior document and that employees with significant security responsibilities receive the appropriate amount of training.

***Agency Response:*** Agreed. We need to re-write the rules of behavior in light of the new guidance and so will start the process over again.

**OIG Response:** *The OIG concurs.*

### 7. Security planning documentation is inconsistent in version control, revisions/updates, and dissemination to required officials.

During our review we encountered several instances of multiple versions of the same security planning documents. Some notable discrepancies identified included:

- Different versions of security documents (e.g. Tech BCP, CRS SSP);

- No noted change records or version control;
- Documents not always updated periodically;
- Disaster Recovery planning and testing not formally documented; and
- ISO position lacks succession planning and points of contact.

Additionally, we noted that while the NCUA network diagrams document the critical access paths to the NCUA network infrastructure, there are some external connections that are not specifically identified. For example, the NCUA network security engineer's remote connection to the network.

The NCUA IT security program is adversely affected by lacking documentation that is formally updated and promulgated to affected officials. In addition, OCIO staffing does not support immediate administrative succession of key personnel to coordinate administrative and operational functions.

The Federal Information Security Management Act provides guidance related to these conditions:

> *Each agency shall develop, document, and implement and agency-wide information security program that supports the operations and assets of the agency…policies and procedures should be based on risk assessments and be cost effective. (Section 301, 3544, a3,D)*

Additionally, NIST Special Publication (SP) 800-53 and SP 800-30 provide guidance related to these conditions:

> *SP 800-53 guides that agencies must plan, develop, and disseminate all plans policies and procedures to facilitate security planning and planning controls.*
>
> *SP 800-30 guides that, when developing information risk assessments, the network topology should be considered. (Section 3.1.1)*

**Recommendation:** We recommend that NCUA management improve its security document management process and formally establish organization staffing, to include contributions and responsibilities of program officials. Additionally, we recommend that NCUA management include specific remote connection information in the existing network diagram, including the NCUA network security engineer's remote connection.

***Agency Response:*** Agreed.

**OIG Response:** *The OIG concurs.*

### 8. E-Authentication risk assessments have not been completed for NCUA systems.

NCUA has not completed E-Authentication risk assessments for its systems. While a formal risk assessment has been completed for four out of six NCUA systems, E-Authentication risk considerations were not specifically addressed. The NCUA has asserted that the requirement to complete an E-Authentication risk assessment does not apply to the agency and therefore has not been completed.

By not completing an E-Authentication risk assessment, the NCUA increases the risk of not complying with OMB policy, and may not fully capture risks associated with their e-Government activities.

OMB, M-04-04, *E-Authentication Guidance for Federal Agencies*, Section 11, requires that:

> *Agencies review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. Additionally, section 1.2 notes, it applies to the remote authentication of human users of Federal agency IT systems for the purposes of conducting government business electronically (or e-government).*

**Recommendation:** We recommend that NCUA management complete the E-Authentication risk assessment process in accordance with OMB Memorandum 04-04, E-Authentication Guidance for Federal agencies.

***Agency Response:*** It has never been our position that NCUA is exempt from the E-Authentication risk assessment requirements. Rather, our position is that these requirements apply to E-Commerce conducted by government agencies, as indicated in the excerpt from OMB Memorandum M-04-04 that you cited above. Our interpretation was confirmed verbally by the cognizant OMB desk officer in a conversation with the NCUA Information Security Officer and then confirmed in writing. Since NCUA does not engage in E-commerce, we have *not triggered* the requirement to conduct an E-authentication risk assessment.

Nonetheless, we have agreed to review the risk assessment template offered by the OIG in order to determine whether we have the need or resources to perform these risk assessments as a matter of good faith.

**OIG Response**: *The OIG acknowledges the agency's position on E-Authentication risk assessments. However, we still recommend that the agency conduct e-authentication risk assessments as required by OMB M-04-04.*

### 9. Security configuration guides are not utilized for NCUA systems.

The NCUA has not established formal security configuration guides for its systems. Security configuration guides establish a security baseline on which to configure systems to ensure a consistent application of security controls. The NCUA has established limited configuration guides for its operating systems. However, guides for firewalls, domain servers, and routers do not formally exist.

By not establishing and implementing a formal security configuration guide, the NCUA increases the risk of not consistently applying security standards across agency information technology resources.

FISMA requires agencies to create secure baseline configurations. Section § 3544 concerning federal agency responsibilities states:

> *(b) AGENCY PROGRAM.—Each agency shall develop, document, and implement an agency wide information security program, approved by the Director under section 3543(a)(5), to provide information security for the information and information systems that support the operations and assets of the agency, including those provided or managed by another agency, contractor, or other source, that includes— …*
>
> *(2) policies and procedures that—*
>
> *(D) ensure compliance with—*
>
> *(i) the requirements of this subchapter;*
>
> *(ii) policies and procedures as may be prescribed by the Director, and information security standards promulgated under section 11331 of title 40;*
>
> *(iii) minimally acceptable system configuration requirements, as determined by the agency;*

**Recommendation:** We recommend that NCUA management establish and implement an agency-wide security configuration policy.

***Agency Response:*** We may be working from two different interpretations of what constitutes a security configuration baseline. Our interpretation defines Windows 2003 out of the box as a configuration baseline along with subsequent changes which are documented in the server build document. We also used this approach with our routers.

***OIG Response:*** *FISMA (section 3544(b)(2)(D)(iii)) requires each agency to develop minimally acceptable system configuration requirements and ensure compliance with them. Systems with secure configurations have fewer vulnerabilities and are better able to thwart network attacks. "Out-of-the-box" settings often lack necessary changes and restrictive settings to minimize vulnerabilities.*

*Under the Cyber Security Research and Development Act of 2002, NIST created the Security Configuration Checklist Program, designed to "develop, and revise as necessary, a checklist setting forth settings and option selections that minimize the security risks associated with each computer hardware or software system that is, or is likely to become widely used within the Federal Government." Under this program, described in NIST SP 800-70, agencies are to use checklists to establish a minimum security configuration for its systems and major applications, which are based on current practices in other Agencies, vendors, consortia and academia.*

### 10. The NCUA Continuity of Operations Plan (COOP) and IT Disaster Recovery procedures are not consistently updated.

The NCUA COOP has not been updated since 2004 and documentation noting an update schedule for the NCUA COOP was not available. According to NCUA proposed updates are being reviewed by the Regional Offices and Central Office for accuracy. The updates were to be completed in approximately 30 days and the core COOP will be revised in 90-120 days. Additionally, no documentation has been provided to demonstrate testing of disaster recovery plans during the current year.

The NCUA *Technical Business Continuity Plan* does not reflect having been consistently updated on an annual basis. In addition, the plan does not appear to have adequate version control for purposes of review and update. The initial version provided was dated 4/21/2005. However on 6/21/2006, we were provided with a version with recent changes that was dated 7/12/2002.

Additionally, we noted that both AMAC Disaster Recovery Plan documents, *(AMAC) Asset Management & Assistance Center: Computer Systems Disaster Recovery Plan* and *Disaster Recovery Plan: Asset Management and Assistance Center* have not been updated since June of 2003.

By not updating the COOP documents, NCUA increases the risk of not being able to recover timely from a service disruption and of not providing pertinent employees with accurate plans, procedures and technical measures to enable the recovery of systems, operations, and data after a disruption.

NIST SP 800-34, *Contingency Planning Guide for Information Technology Systems*, requires all agencies to create, update, and test a contingency plan for major systems:

> *<u>Develop an IT contingency plan.</u> The plan should contain detailed guidance and procedures for restoring a damaged system.*
>
> *To be successful, senior management, most likely the Chief Information Officer (CIO) must support a contingency program. These officials should be included in the process to develop the program policy, structure, objectives, and roles and responsibilities. At a minimum, the contingency policy should comply with federal guidance contained in the documents listed in Section 1.1; agencies should evaluate their respective IT systems, operations, and requirements to determine if additional contingency planning requirements are necessary. Key policy elements are as follows:*
> - *Roles and responsibilities*
> - *Scope as applies to the type(s) of platform(s) and organization functions subject to contingency planning*
> - *Resource requirements*
> - *Training requirements*
> - *Exercise and testing schedules*
> - *Plan maintenance schedule*
> - *Frequency of backups and storage of backup media*
>
> *It is essential that the contingency plan be reviewed and updated regularly, as part of the organization change management process, to ensure new information is documented and contingency measures are revised if required.*

**Recommendation:** We recommend that NCUA management update the NCUA COOP plan, the Technical Business Continuity plan, and the AMAC Disaster Recovery Plan by completing their process conducting annual reviews and revisions.

***Agency Response:*** Agreed.

**OIG Response:** *The OIG concurs.*

### 11. Testing of NCUA Disaster Recovery and system contingency plans does not occur regularly.

Testing of NCUA Disaster Recovery/System Contingency plans does not occur on a routine basis (at least annually) and lack specific policies for conducting periodic testing. Review of the NCUA security program for FY2006 FISMA reporting indicates only one of six systems in the NCUA system inventory have tested contingency plan(s) in the last year. Additionally, the Technical Business Continuity Plan does not reflect updates (at least annually) of test results and plan changes.

By not periodically testing and updating IT System Disaster Recovery (DR) and Contingency plans with lessons learned from the testing potentially impacts the effectiveness of these plans when required for real-world occurrences, and may impact system restoration priorities based on criticality.

NIST 800-53, section CP-4, guides that the information system DR and Contingency plans must be updated frequently, at least annually, and that contingency plan testing is coordinated with other related plans, such as COOP, Incident Response, etc)

**Recommendation:** We recommend that NCUA management develop policies and procedures to test and update DR and Contingency plans at least annually, or more frequently if required.

***Agency Response:*** Mostly agree. We believe that the AMAC system failure and subsequent recovery is a valid test of the DR plan.

**OIG Response:** *The OIG disagrees that the AMAC system failure constitutes a test of the disaster recovery plan. NCUA should test all of its disaster recovery and contingency plans on an annual basis.*

### 12. Restoration priorities related to system impact ratings have not been documented.

NCUA has not documented restoration priorities related to impact ranking to insure systems most critical to NCUA operations are restored according to mission criticality. It is not clear that the current NCUA documentation reflects overall restoration priorities based on system criticality since impact rankings and system categorization for availability were based on impact to the Federal Government vice impact to NCUA operation.

The inconsistent application of FIPS 199 categorization may impact how NCUA reconstitutes IT operations in support of NCUA business requirements.

**Recommendation:** We recommend that NCUA management complete the Business Impact Analysis required and ensure that the priority for restoration of IT systems is consistent with the impact rankings as related to NCUA's mission.

***Agency Response:*** Agreed. We have now implemented consistent FIPS 199 categorization, but this doesn't address NCUA's restoration priorities.

**OIG Response:** *The OIG concurs.*

## 13. NCUA physical security measures are not consistently enforced.

During our evaluation we noted that some physical security measures are not consistently implemented in the NCUA Central Office:

- We requested a copy of a recent physical security risk assessment conducted over NCUA facilities; however, we were informed one had not been completed.
- NCUA procedures do not adequately address the controlled reentry of personnel following an emergency evacuation. The NCUA Facility Self-Protection Plan For 1775 Duke Street describes the reentry procedures following an emergency evacuation; however, these procedures do not specifically account for identity checks in a situation where normal access controls (like locked doors and security guards) are unlikely to be in place.

The lack of a facility risk assessment limits the organizational knowledge of risk and the ability of NCUA to disseminate risk knowledge throughout the organization. By not implementing procedures for identity checking all individuals reentering the Central Office following an emergency evacuation, NCUA increases the risk of “piggybacking” of non NCUA personnel in a mass reentry. This may allow unauthorized access to sensitive NCUA data and facilities. Through inconsistent application of physical access controls, the NCUA increases the risk of unauthorized individuals gaining access to sensitive areas of the Central Office. This may increase the risk to NCUA data confidentiality, integrity, and availability.

NIST SP 800-30 and 800-53 provide guidance to agencies for these conditions.

> *SP 800-30 guides that when developing information risk assessments, the physical security environment of IT systems (e.g., facility security) should be considered. (Section 3.1.1)*
>
> *SP800-53 guides that the organization controls all physical access points (including designated entry/exit points) to facilities containing information systems (except for those areas within the facilities officially designated as publicly accessible) and verifies individual access authorizations before granting access to the facilities. (Section PE-3)*

**Recommendation:** We recommend that NCUA management develop a risk assessment covering the Central Office facility and consistently enforce existing physical security policies. Additionally, we recommend that NCUA management update the Facility Self-Protection Plan with the inclusion of procedures that ensure the prevention of unauthorized personnel during reentry following an emergency evacuation.

***Agency Response:*** Agreed. We will include this item in our POA&M and forward it to DPFM for their action.

**OIG Response**: *The OIG concurs.*

## 14. Periodic incident response training has not been conducted for NCUA personnel.

The NCUA does not conduct regular incident response training for its personnel. Additionally, the incident response plan does not articulate, or provide guidance for training of personnel in their respective roles and responsibilities. Training helps ensure that incident response team members are familiar with NCUA incident reporting practices and can increase the efficiency of a response.

The NCUA utilizes a Rules of Behavior document to disseminate security policies to employees and to document their understanding. However, the current Rules of Behavior document does not specifically give guidance to employees in reporting security incidents. The NCUA Rules of Behavior does not communicate what personnel should report to the Technical Support Desk in the event that a serious incident does occur. Additionally, “security incidents” are not defined in user training and reflected in the user rules of behavior.

By not providing incident response training, NCUA increases the risk of employees not understanding or adhering to the policies and procedures that NCUA has put in place for incident response handling. Additionally, it increases the risk of incident response team members not being fully trained and capable of performing their additional duties.

**Recommendation:** We recommend that NCUA management define “incidents” as part of user training and insure roles and responsibilities are articulated and to review the Rules of Behavior disclosure to assure that clear procedures are articulated to personnel regarding what to report in the event that an incident occurs.

Additionally, we recommend that the NCUA provide additional training to its incident response team members over current best practices and federal guidance.

***Agency Response:*** Agreed.

**OIG Response:** *The OIG concurs.*

### 15. NCUA’s Plan of Actions and Milestones (POA&M) process needs improvement.

NCUA program officials do not actively support the process of tracking and updating the Plan of Actions and Milestones (POA&M) for their respective systems. Based on review of documentation and interviews with the NCUA ISO, the POA&M process is largely driven by updates from the ISO, instead of the ISO receiving periodic updates from program officials responsible for remediation requirements. Program officials are not actively identifying vulnerabilities or weaknesses and incorporating them into existing POA&Ms.

Additionally, while certain risks to the ESS system were known by the NCUA ISO, they were not formally incorporated into the POA&M. The risks not included follow:

- The CIO and ISO have been aware of weaknesses in backups to external drive (lack of encryption of sensitive data)
- Risk Assessment and POA&M does not reflect use and risk of all external storage media in use that contains sensitive data in an unencrypted format. (i.e. CD drives are addressed but not USB drives)

During our inspection of the NCUA POA&M and related documentation, we noted that not all AMAC findings identified from the AMAC certification conducted by the ISO are captured in the NCUA POA&M document such as:

- AMAC personnel accepting credit card or ACH information over the phone for payments from credit union customers could lead to fraud;
- Aftech no longer has modem access to the AMAC system; and
- The computer room does not have a raised floor;

The NCUA ISO faces the additional burden of tracking agency efforts to remediate risk and vulnerabilities by having to actively pursue status updates for program officials for their respective action items. Additionally, by not including critical risks identified for the ESS and AMAC systems, NCUA management may not have a full picture of risks to that system on which to base their certification and accreditation decision.

NIST SP 800-37 states that the authorizing official or designated representative should work with the information system owner to revise the POA&M to ensure that proactive measures are taken to correct security deficiencies in the information system. The POA&M, which is prepared by the information system owner, describes measures that have been implemented or planned to correct deficiencies noted during the assessment of the security controls and reduce or eliminate known vulnerabilities in the information system.

NIST SP 800-37 also states that the POA&M submitted by the information system owner is used by the authorizing official to monitor progress in correcting deficiencies noted during the security certification. In addition to executing the POA&M, information system owners should also establish a disciplined and structured process to monitor the effectiveness of security controls in the information system during the period of limited authorization to operate.

**Recommendation:** We recommend that NCUA management implement and enforce policy that better supports the NCUA ISO in receiving and tracking updates to the POA&M as warranted. In addition, the ISO needs to ensure all identified weaknesses are incorporated into the POA&M.

***Agency Response:*** Agreed.

**OIG Response**: *The OIG concurs.*