# NATIONAL CREDIT UNION ADMINISTRATION
# OFFICE OF INSPECTOR GENERAL

**INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 2009**

**Report #OIG-09-02** **October 16, 2009**


*William A. DeSarno*
*Inspector General*

***Released by:***

*James Hagen*
*Deputy IG for Audits*

***Auditor-in-Charge:***

*W. Marvin Stith, CISA*
*Sr Information Technology Auditor*

## Contents

# I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged Richard S. Carson and Associates, Inc (Carson Associates), to independently evaluate 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.

Carson Associates evaluated NCUA's security program through interviews, documentation reviews, technical configuration reviews, an after-hours walk-through, and sample testing. We evaluated NCUA against standards and requirements for federal government agencies such as those provided through FISMA, the Government Accountability Office's *Federal Information System Controls Audit Manual* (FISCAM), National Institute of Standards and Technology (NIST) Special Publications (SPs), and Office of Management and Budget (OMB) memoranda. We conducted an exit conference with NCUA on July 15, 2009, to discuss evaluation results.

The NCUA has worked to further strengthen its information technology (IT) security program during Fiscal Year (FY) 2009. NCUA's accomplishments during this period include:

- Installation of a change control management system for its IT systems;
- Improved employee enter/exit procedures;
- Enhanced policies and procedures;
- Improved contingency plan testing;
- Completed re-certification of a major certification & accreditation (C&A) package;
- Currently undergoing a re-certification of one major C&A package;
- Improved plan of action and milestones (POA&M) process; and
- Completed control testing for all six systems

We identified five areas remaining from last year's FISMA evaluation that NCUA officials need to address:

- Improve its vulnerability management procedures;
- Implement continuing education requirements for its information technology (IT) employees;
- Establish adequate segregation of duty controls for its applications;
- Complete e-authentication risk assessments for its FISMA systems; and
- Improve its contingency planning program for its FISMA systems.

In addition, we identified 10 new findings this year where NCUA could improve IT security controls. Specifically, NCUA needs to:

- Improve its security configuration program;
- Enhance its procedures for ensuring terminated users and inactive user accounts are removed from its systems;

- Improve its System Software Change Procedures;
- Incorporate specific security and response time requirements into the Service Level Agreement (SLA) for its Intrusion Detection System (IDS);
- Improve its remote access controls;
- Enhance its information privacy and security awareness program;
- Update its web site privacy policy;
- Improve its process for certifying its FISMA systems;
- Complete its FY2009 security awareness training; and
- Complete an Authorization to Operate for one of its FISMA systems.

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. The Federal Information Security Management Act (FISMA) permanently reauthorized the framework laid out in the Government Information Security Reform Act of 2000 (GISRA), which expired in November 2002. FISMA continues the 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 2009 Reporting Instructions for the Federal Information Security Management Act on August 20, 2009. This document provides clarification to agencies for implementing, meeting, and reporting FISMA requirements to OMB and Congress.

## National Credit Union Administration (NCUA)

NCUA is the independent federal agency that charters, supervises, and insures the nation's federal credit unions. NCUA 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 of Directors (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 two board members can be from the same political party, and each member serves a staggered six-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 audit 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. We evaluated NCUA's efforts related to:

- Efficiently and effectively managing its information security program;
- Meeting responsibilities under FISMA;
- Remediating prior audit weaknesses pertaining to FISMA and other security weaknesses identified; and
- Implementing its plans of action and milestones (POA&M)

In addition, 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

We evaluated NCUA's information technology (IT) security program and practices against such standards and requirements as those provided through FISMA, the Government Accountability Office's *Federal Information System Controls Audit Manual* (FISCAM), National Institute of Standards and Technology (NIST) Special Publications (SPs), and Office of Management and Budget (OMB) memoranda.

We review IT security control techniques for all of NCUA's major information systems on a rotational basis. During this evaluation, we assessed NCUA's controls over security planning and program management, segregation of duties, privacy and security awareness training, physical and logical access, and incident response. In addition, we evaluated areas required to report under OMB M-09-29, such as reviews of privacy and breach notification, certification and accreditation (C&A) documentation including system security plans, risk assessments, contingency plans, and certification reports. Furthermore, we reviewed existing IT security controls and identified weaknesses impacting certain general support system (GSS) components, application security (to include change controls and configuration management), and service continuity.

We conducted our fieldwork from May 2009 through October 2009. We performed our audit in accordance with generally accepted government auditing standards (GAGAS), audit standards promulgated by the 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. NCUA has made progress in addressing last year's reported deficiencies; however, some prior year deficiencies remain. In addition, we identified other areas for improvement that require management's attention. We discuss these issues below.

### 1. NCUA needs to improve its security configuration program.

NCUA has established a configuration guide for its workstation and server operating systems. However, NCUA has not documented its compliance with or variances from NIST baseline security configurations for its workstations. In addition, NCUA has not implemented the NIST-approved security configurations for its servers and network devices (e.g., routers, switches, firewalls etc). Furthermore, NCUA has not implemented a procedure and tool to verify its workstations, server and network device configurations against the NIST baseline security configurations.

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them.[1] OMB Memorandum M-07-11 directed agencies using Windows XP or planning to upgrade to the Vista operating system, to adopt OMB-mandated Federal Desktop Core Configuration (FDCC) security configurations. In addition, OMB Memorandum M-08-22 requires:

- Industry and government information technology providers to use Security Content Automation Protocol (SCAP)[2] validated tools with FDCC Scanner capability to certify that their products operate correctly with FDCC configurations and do not alter FDCC settings.

- Agencies to use SCAP tools to scan for both FDCC configurations and configuration deviations approved by department or agency accrediting authority.

- Agencies to use SCAP tools when monitoring the use of these configurations as part of FISMA continuous monitoring.

NIST has made available through the National Checklist Program[3], security configuration checklists[4] for operating systems and applications that are widely used

[1] Section 3544(b)(2)(D)(iii)).
[2] SCAP enables validated security tools to perform automatic configuration checking using NCP checklists within this category.
[3] The National Checklist Program is the U.S. government repository of publicly available security checklists (or benchmarks) that provide detailed low level guidance on setting the security configuration of operating systems and applications.

within the Federal Government. NIST encourages agencies to implement the applicable checklists into their environment and document any deviations from the common security configurations with justifications.

NCUA upgraded its workstation operating system to Vista in early 2009. NCUA's configuration guide requires configuring agency workstations following the OMB-mandated Federal Desktop Core Configuration (FDCC) security configurations. However, while NCUA officials indicated they implemented FDCC security configurations (with variances), NCUA has not documented its compliance with and variances from the baseline FDCC configurations.

In addition, NCUA has not implemented the applicable NIST security checklists provided under the National Checklist Program to configure its servers and network devices. NCUA indicates it uses the Microsoft Baseline Security Analyzer (MBSA) to provide a baseline security configuration for and verify the configurations of its servers. However, the MBSA relies solely on Microsoft's recommended security settings and is not an approved SCAP tool with Authenticated Configuration Scanner Capabilities. In addition, NCUA manually configures its network devices and stores the baseline configurations locally. However, NCUA does not use NIST baseline security configuration guidelines for the devices or an SCAP scanner with Authenticated Configuration Scanner capabilities to ensure compliance of the network devices with the baseline configurations.

NCUA officials indicated they have not implemented the National Checklist Program for its servers due to IT staff resource constraints and additional security priorities taking precedence. However, NCUA officials indicated they are evaluating approved SCAP tools. By not adopting the NIST-approved server security configuration checklist, NCUA is not implementing federally accepted server security standards. In addition, by not using SCAP validated tools, NCUA cannot appropriately validate the implementation of the National Checklist Program on its workstations, servers and network devices.

**Recommendation 1:** We recommend that NCUA:

1) Select and implement a Security Content Automation Protocol (SCAP) validated vulnerability scanner/appliance with Federal Desktop Core Configuration (FDCC) Scanner and Authenticated Configuration Scanner capabilities;

2) Verify FDCC security configurations for its workstations using the FDCC scanner capabilities and document the deviations; and

[4] A security configuration checklist essentially contains instructions or procedures for configuring an IT product to a baseline level of security. A checklist might include: (a) Configuration files that automatically set various security settings; (b) Documentation that guides the checklist user to manually configure software; (c) Documents that explain the recommended methods to securely install and configure a device; and (d) Policy documents that set forth guidelines for such things as auditing, authentication security, and perimeter security.

3) Implement and verify NIST baseline security configurations for servers and network devices using the Authenticated Configuration Scanner capabilities and document the deviations.

***Agency Response:*** *NCUA agrees with the recommendations and would like to note that this finding has no impact on the actual security of NCUA systems.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions. The OIG also notes that by using and verifying the common NIST configurations, NCUA will be helping improve security, reduce costs, and decrease application-compatibility issues among and across federal government agencies.

## 2. NCUA needs to improve its vulnerability management procedures.

This finding pertains to a FY 2007 finding which indicated a deficiency in the NCUA vulnerability management program, noting a number of ports/communication services were available on specific NCUA servers. This finding was repeated in FY 2008.

NIST Special Publication (SP) 800-53, Revision 2 guides that organizations conduct an assessment of the security controls in the information system to determine the extent to which the controls are implemented correctly, operating as intended, and producing the desired outcome with respect to meeting security requirements of the system. NIST SP 800-53 also guides that the organization:

- Periodically scan for vulnerabilities in the information system and scan the system when significant new vulnerabilities potentially affecting the system are identified and reported.
- Employ vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  - Enumerating platforms, software flaws, and improper configurations;
  - Formatting and making transparent, checklists and test procedures; and
  - Measuring vulnerability impact.
- Analyze vulnerability scan reports and remediate legitimate vulnerabilities and organizational assessment of risk.
- Share information obtained from the vulnerability scanning process with designated personnel throughout the organization to help eliminate similar vulnerabilities in other information systems.

NCUA has implemented Microsoft's System Center Configuration Manager (SCCM) with Windows Server Update Services (WSUS) to act as patch-level compliance

software, and SolarWinds software to perform port scanning weekly until a vulnerability scanner appliance is installed. However, NCUA has not fully implemented a comprehensive vulnerability management process to include vulnerability scanning, reporting, and remediation.

NCUA officials indicated they are in the process of evaluating vulnerability scanners/appliances and creating procedures to implement the vulnerability scanning process with an expected completion date before the end of FY 2009. Although NCUA is currently scanning patch levels and open ports with SCCM, WSUS, and SolarWinds software, these tools do not test for vulnerabilities with services running on the open ports, misconfigurations, and other vulnerabilities in the environment (i.e., web applications, databases, etc). Therefore, NCUA's current processes do not provide NCUA with a comprehensive vulnerability management process, which may increase the risk of an unauthorized person gaining access to NCUA systems through exploitation of unknown vulnerabilities.

**Recommendation 2:** We recommend that NCUA implement procedures to continuously monitor open ports and services on NCUA servers and address vulnerabilities.

***Agency Response:*** *NCUA agrees and is working on implementing a solution.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions.

### 3. NCUA needs to implement continuing education requirements for its information technology (IT) employees.

NCUA has not established training requirements for its IT employees or a mechanism to effectively track and report the training taken. This is a repeat finding from the FY 2007 and FY 2008 FISMA evaluations.

NIST SP 800-53, Revision 2, guides that organizations provide system managers, system and network administrators, and other personnel having access to system-level software with adequate technical training to perform their assigned duties. It also guides that the organization document and monitor individual information system security training activities including basic security awareness training and specific information system security training. In addition, the NCUA Agency Wide Information Security Policy indicates that training oversight includes general awareness training and specific training for people with significant security responsibilities. The policy requires the CIO to ensure adequate training is planned for NCUA.

In response to our FY 2008 FISMA recommendations:

- OCIO officials agreed to establish and document continuing education requirements for IT employees in each employee's Individual Development Plan.

- OHR officials indicated that by April 2009, they would implement the web-based Learning Management System (LMS) to monitor and track employee training records.

We determined that while OCIO managers indicated they were researching training for their IT employees, they have not established or documented continuing education requirements. In addition, OHR officials indicated that due to delays with the system provider and internal resource constraints, they were unable to meet the planned completion date. The officials indicated they anticipated beginning to implement the LMS in August 2009, with full implementation expected by September or October 2009.

By not establishing continuing education requirements and requiring specific security-related training for its IT employees, NCUA cannot ensure the IT employees have the most current technical knowledge to effectively protect the confidentiality, integrity, and availability of its systems and sensitive data.

**Recommendation 3**: We recommend that NCUA:

1) Establish continuing education requirements for its information technology employees.

2) Complete its implementation of the Learning Management System.

***Agency Response:*** *Current policies rely on each OCIO manager's discretion to determine the security training required by employees with significant security responsibilities. This is determined each year and documented using the Individual Development Plan (IDP) process. This process effectively meets the changing security training requirements OCIO faces each year. In order to make this process more robust, the agency will require a meeting of managers at the beginning of each IDP cycle to establish that year's security training requirements. These requirements will be documented and stored with the security plan. This finding has minimal impact on the actual security of NCUA systems. The Division of Training and Development anticipates the Learning Management System will go live by the end of October 2009.*

*Estimated completion date for item #1: 5/1/2010*
*Estimated completion date for item #2: 10/31/2009*

**OIG Response:** The OIG concurs with NCUA's planned actions.

### 4. NCUA needs to enhance its procedures for ensuring terminated users and inactive user accounts are disabled or removed from NCUA and external systems.

We identified active user accounts for terminated NCUA employees on some NCUA and external systems. In addition, we identified inactive accounts for current NCUA employees on an NCUA system.

NIST SP 800-12 indicates when user accounts are no longer required, the supervisor should inform the application manager and system management office so accounts can be removed in a timely manner. In addition, NIST SP 800-53, Revision 2, guides that organizations:

- Develop, disseminate, and periodically review/update formal, documented procedures to facilitate the implementation of the access control policy and associated access controls.

- Manage information system accounts, including establishing, activating, modifying, reviewing, disabling, and removing accounts.

In response to our FY2008 FISMA review, NCUA updated its employee enter/exit/change procedures effective May 2009 to facilitate the timely removal of terminated employees' user accounts. In addition, OCIO staff informed us that they implemented a new process in June 2009 to review and disable inactive Active Directory user accounts on a weekly basis. We reviewed the listing of terminated NCUA employees against NCUA's system account listings and determined that seven terminated employees had active user accounts on NCUA and external systems. We also identified two user accounts for current employees on one of NCUA's systems, which have been inactive for over two years.

We determined that for all but one employee, NCUA's new enter/exit/change procedures were not in effect when the terminated employees left the agency prior to May 2009. For the one remaining employee who left the agency in June 2009, we determined NCUA had not appropriately included in the email notification distribution list the person responsible for adding/removing/changing the user's access for that system. Also, while NCUA implemented a new process to review and disable inactive Active Directory user accounts, NCUA has not formalized/documented the process. Furthermore, the process did not identify the inactive user accounts because the process only applies to reviewing Active Directory user accounts on the GSS, and the inactive user accounts were not on the GSS.

By not disabling inactive user accounts and not removing the access of terminated employees in a timely manner, existing and former employees may use these accounts to obtain unauthorized access to sensitive NCUA data. In addition, NCUA should formally document the user account review process to institutionalize and help ensure the continuity and consistent execution of the process within NCUA.

**Recommendation 4:** We recommend that NCUA:

1) Update the enter/exit/change procedures email notification distribution list to include appropriate personnel for external systems and review this list periodically to ensure the list remains current.

2) Document the process for reviewing and disabling inactive user accounts on a weekly basis.

3) Include in the process of reviewing and disabling inactive user accounts, the requirement to review user accounts on network devices and external systems.

4) Review Active Directory accounts and external system user accounts to identify and remove accounts for employees terminated prior to May 13, 2009.

***Agency Response:*** *NCUA agrees with the recommendation. OCIO and OHR will implement the necessary solutions.*

*Estimated completion date: 12/31/2009*

**OIG Response:** The OIG concurs with NCUA's planned actions.

### 5. NCUA needs to improve its System Software Change Procedures.

NCUA has implemented procedures to ensure that information required for a system software change request/notification is adequately and properly documented. However, NCUA has not incorporated these procedures into its formal system software change control policies and procedures. In addition, NCUA has not established change controls for its Commercial Off-The-Shelf (COTS) software.

NIST SP 800-53, Revision 2, guides that the organization:

- Develop, disseminate, and periodically review/update a formal documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance.

- Authorize, document, and control changes to the information system.

In addition, the FISCAM indicates that a disciplined approach for testing and approving new and modified programs prior to their implementation is essential to make sure programs operate as intended and that no unauthorized changes are introduced.

NCUA implemented Microsoft SharePoint to document change requests for system software components to ensure that all changes are properly documented and approved. We determined the change requests are sufficiently detailed and include the appropriate approvals. However, NCUA has not updated its official change management policies and procedures for its system software to mirror current practice. In addition, NCUA does not have change control procedures for COTS software.

NCUA officials indicated they have not updated the change management policies and procedures due to IT staff resource constraints and additional security priorities taking precedence. By not updating its current change management policies and procedures to mirror current practice, NCUA increases the risk that NCUA staff may inadvertently follow the old procedures resulting in unauthorized changes being made to NCUA systems. In addition, by not establishing change control procedures for COTS software, NCUA risks the potential loss of the confidentiality, availability, and integrity of the data in its COTS systems.

**Recommendation 5:** We recommend that NCUA

1) Update its system software change control policies and procedures to reflect the current process.

2) Establish and document COTS change control policies and procedures.

***Agency Response:*** *NCUA agrees with both recommendations. OCIO has already addressed these recommendations through replacement of the old procedures in the OCIO security plan with the following text:*

> ***3.5.1 Common Controls***
>
> ***Authorization***
> - *All changes to the production network, servers, systems, and applications will be documented by submitting a Configuration Change Request form. This form is available on OCIO's site within NCUACentral....*
>
> - *This procedure applies to all staff in the Division of Systems and Technical Support and Division of Product Services, including all contractor staff.*
>
> - *Changes to the production network are not allowed until the Configuration Change Request form has been approved.*
>
> - *The Configuration Change Request form must provide sufficient detail to thoroughly document the proposed change.*
>
> - *In the case of changes to COTS software, the change must follow the instructions supplied by the vendor. Any deviations to this rule must be documented and will be addressed on a case-by-case basis.*

- *There are four types of change requests as listed below. Use your best judgment in choosing the type for your requested change.*

    - ***Informational*** *- The change is routine and does not require explicit authorization by a Division Director. An information period of 12 hours must elapse before this change request is automatically approved to allow time for review and comment by the configuration control distribution list. The change may not proceed until this period has elapsed, nor may it proceed if comments are received until those comments are resolved.*

    - ***Authorization*** *- Both Division Directors must authorize the change before it can be implemented. Also, an information period of 24 hours must elapse before this change request is approved to allow time for review and comment by the configuration control distribution list. The change may not proceed until this period has elapsed and both division directors have approved the change, nor may it proceed if comments are received until those comments are resolved.*

    - ***Emergency*** *- This is where the CIO, Deputy CIO, or person acting on their behalf has directed you to make a change right away. Division Directors may not authorize emergency changes. If possible, submit the Configuration Change Request form prior to implementing the change.*

    - ***Committee*** *- This change is extensive or involves significant architectural changes to the production network. Such changes warrant review by the Change Control Committee and approval by both Division Directors before proceeding. Brand new systems or applications would be examples warranting review by the Change Control Committee.*

*Examples of changes warranting configuration control:*

- *Any change to a production system, except those listed in the exceptions below,*
- *Hardware upgrades,*
- *Operating system upgrades and Service Packs,*
- *Software upgrades and/or changes,*
- *Firewall configuration changes,*
- *Switch and router configuration changes,*
- *Changes to laptop configuration including SMS updates.*

*Exceptions to this policy:*

- *Developmental servers, systems, and applications running in the development environment do not require a Change Request form,*
- *Changes resulting from an employee add/change/exit action,*

- *Hot-fixes and patches to the Windows OS on production systems,*
- *Internet or Intranet web (HTML) content changes,*
- *E-Library changes.*
- *Internet or Intranet web (HTML) content changes,*
- *E-Library changes.*

**OIG Response:** The OIG concurs with NCUA's action.

### 6. NCUA needs to establish adequate segregation of duty controls[5] for its applications.

NCUA has begun to take steps to remedy the segregation of duties issues with its applications; however, NCUA has not fully addressed the recommendations from prior year FISMA reviews. This finding pertains to a FY 2007 finding, which was repeated in the FY 2008 FISMA evaluation.

NIST SP 800-53, Revision 2, indicates that information systems should enforce segregation of duties through assigned access authorizations. The organization should establish appropriate divisions of responsibility and separate duties as needed to eliminate conflicts of interest in the responsibilities and duties of individuals.

NCUA does not have adequate controls for segregation of duties in place for its applications. Specifically, we determined that NCUA has not addressed the following findings from our 2008 FISMA review:

- Programmers for three of NCUA's FISMA systems were improperly authorized access to both development and production application environments.

- A single administrator of NCUA's financial system had sole responsibility for managing system operations in the systems production environment.

- One senior programmer had access to all of the NCUA production environments without documented justification or compensating controls.

- NCUA had not documented and implemented policy and procedures enforcing periodic supervisory review and monitoring of programmer activities.

In response to these previous findings, NCUA agreed to implement our recommendations to resolve these issues. However, while NCUA officials indicated they are in the process of implementing the recommendations, they are not complete.

[5] Segregation of duties is the practice of dividing the steps in a critical function among different individuals. For example, one system programmer can create a critical piece of operating system code; while, another authorizes its implementation. Such a control keeps a single individual from subverting a critical process.

By not restricting programmer access to production environments and not monitoring systems with limited or non-existent segregation of duties, NCUA increases the risk that intentional or unintentional error, alteration, or deletion of data within its systems may occur. This could negatively impact NCUA by affecting the quality and accuracy of the data it provides to its customers and its examiners.

**Recommendation 6:** We recommend that NCUA:

1) Examine existing roles and responsibilities of all OCIO programmers/computer specialists/SAP administrators and define residual risks associated with segregation of duties conditions created by organizational constraints.

2) Establish and implement compensating controls if segregation of duties conflicts cannot be easily resolved.

***Agency Response:*** *NCUA agrees and is in the process of implementing these recommendations.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions.

### 7. NCUA needs to complete e-authentication risk assessments[6] for its FISMA systems.

NCUA has not specifically addressed e-authentication risk considerations. This is a repeat finding from the FY 2006, FY 2007, and FY 2008 FISMA evaluations.

OMB Memorandum M-04-04 requires agencies to conduct e-authentication risk assessments specifically to review new and existing electronic transactions to ensure that authentication processes provide the appropriate level of assurance. In addition, the guidance applies to the remote authentication of human users of federal agency IT systems for the purposes of conducting government business electronically.

While NCUA has completed formal risk assessments for its six FISMA systems, NCUA did not specifically address e-authentication risk considerations. NCUA officials indicated they have not completed e-authentication risk assessments due to IT staff resource constraints and additional security priorities taking precedence. NCUA officials also indicated that the recommendation is currently in the process of being completed, but is past NCUA's stated completion date of June 1, 2009. By not

[6] An e-authentication risk assessment identifies key user roles and transactions within the application; organizes consequences of false positive authentication and impacts to the agency; and aids in mapping the application to a set of pre-defined authentication criteria by aligning each transaction to a consequence level.

completing e-authentication risk assessments, the NCUA is not compliant with OMB policy.

**Recommendation 7:** We recommend that NCUA complete the e-authentication risk assessment process in accordance with OMB Memorandum 04-04, E-Authentication Guidance for Federal Agencies.

***Agency Response:*** *NCUA agrees and would like to note that this finding has no impact on the actual security of NCUA systems.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions. The OIG also notes that by conducting e-authentication risk assessments in accordance with OMB requirements, NCUA will meet OMB's goal of ensuring that there is a consistent authentication process across the federal government that provides the appropriate level of assurance about user identities presented electronically on information systems.

### 8. NCUA needs to incorporate specific security and response time requirements in the Service Level Agreement (SLA) for its Intrusion Detection System (IDS).

NCUA has a formal SLA with its IDS provider. However, the SLA does not describe specific security and response time requirements the service provider must meet including adherence to OMB, FISMA, NIST, and US-CERT (United States Computer Emergency Readiness Team) requirements.

NIST SP 800-53, Revision 2, guides that the organization: (i) require providers of external information system services to employ adequate security controls in accordance with applicable laws, Executive Orders, directives, policies, regulations, standards, guidance, and established service-level agreements; and (ii) monitor security control compliance.

NCUA officials and the IDS service provider indicated that they have not formally incorporated specific security considerations and response times in the SLA because the service was purchased through a grandfathered GSA schedule agreement. By establishing specific security considerations and response time requirements in the SLA that the service provider must meet, NCUA can help ensure that it will meet the reporting requirements of OMB, NIST, FISMA, and US-CERT.

**Recommendation 8:** We recommend that NCUA update the Service Level Agreement with its Intrusion Detection System service provider to define the necessary security and response time requirements, as mandated by OMB, the National Institute Standards and Technology, FISMA, and the United States Computer Readiness Team.

***Agency Response:*** *The current intrusion detection service is under review for possible replacement. If we keep the current system past the end of the year, we will establish an SLA with the current vendor.*

*Estimated completion date: 12/31/2009*

**OIG Response:** The OIG concurs with NCUA's planned actions.

### 9. NCUA needs to improve its remote access controls.

While the NCUA remote access timeout feature is enabled, the setting exceeds OMB requirements. In addition, NCUA administrators used a shared account to log into the virtual private network (VPN) concentrators, which regulates remote access to the NCUA network.

OMB Memorandum M-07-16, Attachment 1, Section C, *Security Requirements*, requires that organizations use a time-out function for remote access and mobile devices requiring user re-authentication after 30 minutes of inactivity. Also, NIST SP 800-53, Revision 2, guides that all information systems uniquely identify and authenticate users (or processes acting on behalf of users).

NCUA's remote access time-out function is currently set to allow 300 minutes of inactivity before it disconnects. In addition, the VPN concentrators have a generic administrator account that multiple administrators share using a common password.

NCUA management indicated that the extended inactivity time limit on its VPN connection is necessary to perform system updates to the majority of NCUA staff who work remotely. NCUA management noted that many remote users access the VPN using a slower connection. Therefore, the required 30 minute inactivity time is not sufficient for NCUA to provide updates to the users. NCUA management explained that they believe the risk exposed by the current remote access inactivity time setting is mitigated by the mandatory NCUA screen saver function which is set to lock access to the computer after 15 minutes. In addition, NCUA officials indicated that the generic account was a default account used on the VPN concentrator as a backup to the individual user accounts. However, we observed that it became common practice for the administrators to use the generic account because it contained all administrator rights. NCUA officials disabled the generic account during our review; therefore, we are not making a recommendation regarding this issue.

Limiting the remote access inactivity time-out function to meet OMB requirements helps reduce the exposure of NCUA's remote access connections to malicious users who may try to exploit potential vulnerabilities. In addition, accounts shared by more than one user cannot uniquely identify, authenticate, and log the personnel accessing the account. Therefore, audit and accountability controls would not be effective on the VPN concentrators. Consequently, it would be difficult for NCUA officials to identify which

administrator was accountable for authorized, but more importantly, unauthorized configuration changes to the VPN concentrator.

**Recommendation 9:** We recommend that NCUA:

1) Adjust the remote access inactivity time-out function on its VPN concentrators to 30 minutes.

2) Perform a review of all accounts on all systems and network devices to determine if other shared accounts exist and periodically review the systems in the future.

***Agency Response:*** *OCIO will attempt to implement a 60 minute inactivity time-out setting with a pop-up banner that warns the user that the connection will be dropped. Existing compensating controls will mitigate any residual risk.*

*NCUA agrees regarding #2*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG re-emphasizes that NCUA's planned actions do not meet the OMB requirement to implement an inactivity time-out function of 30 minutes. However, the OIG also noted during the review that one of NCUA's compensating controls is an access lock-out screen saver on its remote devices that requires users to re-authenticate to the device after 15 minutes of inactivity.

### 10. NCUA needs to enhance its information privacy and security awareness program.

NCUA conducts annual computer security awareness training and certification to address the privacy and security of electronic information. However, NCUA's information privacy and security training program is not comprehensive.

OMB Memorandum M-07-16 requires that agencies initially train employees (including managers) on their privacy and security responsibilities before permitting access to agency information and information systems. Thereafter, agencies must provide at least annual refresher training to ensure employees continue to understand their responsibilities. Both initial and refresher training must include acceptable rules of behavior and the consequences when the rules are not followed. OMB Memorandum M-07-16 also requires that agencies ensure all individuals with authorized access to Personally Identifiable Information (PII) and their supervisors sign at least annually a document clearly describing their responsibilities.

NCUA's information privacy and security program does not provide for annual training and awareness on the privacy and security of non-electronic information. In addition,

NCUA does not require employees with access to PII (electronic or non-electronic) and their supervisors to annually certify their responsibilities.

NCUA was not aware of OMB's requirements (1) to provide annual privacy and security training on all forms of information, or (2) to have employees and managers with access to PII to annually certify their responsibilities. By providing its employees with annual privacy and security training on all forms of information and requiring applicable employees and their managers to certify their PII responsibilities, NCUA can help ensure all employees who maintain, collect, use, or disseminate electronic and non-electronic information and PII will take necessary precautions to mitigate the unintentional disclosure of sensitive personal information. For example, the OIG conducted an after-hours walkthrough during this review. We found unsecured sensitive information, including PII in several offices and cubicles. The documents were either left out on individuals' desks or the keys to access locked desks and cabinets containing sensitive information were unsecured.

**Recommendation 10:** We recommend that NCUA establish an information privacy and security awareness program, which requires:

1) NCUA to train its employees annually on their privacy and security responsibilities for non-electronic information; and

2) Employees with authorized access to personally identifiable information (and their supervisors) to sign that they understand their responsibilities for that information.

***Agency Response:*** *NCUA has conducted on-line, annual computer security awareness training for employees. In addition, over the last two years, NCUA updated the agency's Privacy Act of 1974 instruction and provided Privacy Act training to all employees at management and regional conferences and through live video training for employees not included in the conferences. Staff recognizes the deficiency as far as providing comprehensive privacy and security training for both electronic and non-electronic formats under FISMA. The annual computer security awareness training has now been revised and enhanced to include training on information privacy and security. This training will be completed for all employees by 10-31-2009. Staff will develop, potentially as part of the IDP or annual appraisal process or as part of the Learning Management System, a means for employees with access to PII and their supervisors to certify that they understand their responsibilities.*

*Estimated completion date for part 1: 10/31//2010*
*Estimated completion date for part 2: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions.

## 11. NCUA needs to update its web site privacy policy.

The NCUA.GOV web site privacy policy is not translated into a standardized, machine-readable format[7], such as the Platform for Privacy Preferences Project Protocol[8] (P3P).

Office of Management and Budget (OMB) Memorandum M-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002*, requires federal agencies to post privacy policies on agency web sites used by the public and translate the policies into a standardized, machine-readable format.

NCUA officials indicated they have not updated the NCUA.GOV web site to include its privacy policy in a standardized, machine-readable format due to IT staff resource constraints and additional security priorities taking precedence. By translating its web site privacy policies into a standard, machine-readable format, NCUA can ensure that the web site privacy policies can be read across multiple types of browsers. This will not only help ensure users are informed of web site privacy practices, but will also ensure browser-based automated decision-making based on these practices, such as accepting cookies, when appropriate.

**Recommendation 11:** We recommend that NCUA:

1) Translate the privacy policies on NCUA.GOV into a standardized, machine-readable format.

2) Review other NCUA web sites and translate the privacy policies into a standardized, machine-readable format.

***Agency Response:*** *NCUA agrees and would like to note that this finding has minimal impact on the actual security of NCUA systems.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions.

[7] A machine-readable format can be scanned or otherwise accessed directly by a computer.
[8] The Platform for Privacy Preferences Project (P3P) enables web sites to express privacy practices in a standard format that can be retrieved automatically and interpreted easily by user agents (e.g., web browsers). P3P user agents will allow users to be informed of site practices (in both machine- and human-readable formats) and to automate decision-making based on these practices when appropriate. Therefore, users need not read the privacy policies at every site they visit.

## 12. NCUA needs to improve its process for certifying its FISMA systems.

NCUA does not conduct an independent assessment of the security controls on four of its six FISMA systems.

NIST SP 800-53, Revision 2, guides organizations with "moderate" or "high" information systems to employ an independent certification agent or certification team to conduct an assessment of the security controls in the information system. Also, NIST SP 800-37 indicates that to preserve the impartial and unbiased nature of the security certification, the certification agent should be in a position that is independent from the persons directly responsible for the development of the information system and the day-to-day operation of the system. The certification agent should also be independent of those individuals responsible for correcting security deficiencies identified during the security certification. The independence of the certification agent is an important factor in assessing the credibility of the security assessment results and ensuring the authorizing official receives the most objective information possible in order to make an informed, risk-based accreditation decision.

We noted that NCUA's own Information Security Officer[9] (ISO) certified four of its six FISMA systems categorized as "moderate". NCUA indicated that the ISO is performing the certification duties due to IT staff resource constraints. However, using an independent agent to certify all of its FISMA systems categorized as "moderate" or "high" will help ensure NCUA's authorizing official[10] receives the most objective information possible in order to make an informed, risk-based accreditation decision.

**Recommendation 12:** We recommend that NCUA employ an independent certification agent or certification team to conduct an assessment of the security controls in NCUA information systems categorized as "moderate" or "high."

***Agency Response:*** *NCUA agrees and plans to let the current certifications stand until it is time for re-certification. At that time, there will be two large systems instead of six smaller ones. (The Office of Examination and Insurance systems --CRS, IIS, and ESS—will be annexed in the GSS.) NAS will be out-sourced by that time, leaving AMAC and the new GSS as the only systems. The Agency will contract with an independent certification agent to certify these two systems. The agency-wide security plan will be updated to reflect these changes.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions.

[9] An information security officer is responsible for setting an agency's overall security policy.
[10] The authorizing official is a senior management official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk to agency operations, agency assets, or individuals.

## 13. NCUA needs to complete its FY2009 security awareness training.

While NCUA has an information security awareness program, it has not provided security awareness training to NCUA employees and contractors for FY 2009.

NIST SP 800-53, Revision 2, guides that organizations provide basic security awareness training to all information system users (including managers and senior executives) before authorizing access to the system, when required by system changes, and thereafter. Also, NIST SP 800-50 provides that agencies must establish an effective security awareness and training program to ensure that users are appropriately trained in the rules of behavior for the systems and applications to which they have access.

NCUA has not initiated and completed its security awareness training to its employees and contractors. NCUA officials informed us they are updating the security awareness training and planned to deploy it to employees and contractors in July 2009 with a planned completion by September 2009. When NCUA completes its security awareness training, it will help ensure employees and contractors mitigate the risks that NCUA systems will be exposed to vulnerabilities that put confidentiality, integrity, and availability of NCUA systems and sensitive data at risk.

**Recommendation 13:** We recommend that NCUA complete its FY 2009 annual security awareness training of all employees and contractors.

***Agency Response:*** *NCUA agrees.*

*Estimated completion date: 10/31/2009*

**OIG Response:** The OIG concurs with NCUA's planned action.

## 14. NCUA needs to complete an Authorization to Operate for one of its information systems.

While NCUA has current Authorizations to Operate (ATO)[11] on five of its six FISMA systems, the agency does not have an ATO for the remaining information system.

NIST SP 800-53, Revision 2, guides that organizations authorize (i.e., accredit) their information system for processing before operations and update the authorization at least every three years or when there is a significant change to the system. A senior organizational official signs and approves the security accreditation. In addition, NIST 800-37 indicates the authorizing official can also: (i) issue an interim authorization to

[11] After assessing the results of the security certification, the authorizing official determines that the risk to agency operations, agency assets, or individuals is acceptable and issues an authorization to operate for the information system. The authorizing official authorizes the information system without any significant restrictions or limitations on its operation.

operate[12] the information system under specific terms and conditions; or (ii) deny authorization to operate the information system (or if the system is already operational, halt operations) if unacceptable security risks exist.[13]

We noted NCUA does not have an ATO for its GSS because it expired this year: NCUA officials indicated that the parties involved in certifying and accrediting the system are still in the process of addressing findings. Therefore, NCUA has not been able to sign the ATO, which allows NCUA to attest that the risk(s) the systems may present, if any, to its operations, assets, or individual are acceptable. However, NCUA officials indicate they have an interim authority to operate.

**Recommendation 14:** We recommend that NCUA complete the certification and accreditation process for the general support system and issue the Authorization to Operate as soon as possible.

***Agency Response:*** *NCUA agrees. OCIO staff is currently working on completing the GSS certification and accreditation.*

*Estimated completion date: 5/1/2010*

**OIG Response:** The OIG concurs with NCUA's planned actions.

### 15. NCUA needs to improve its contingency planning program for its FISMA systems.

NCUA does not have policies and procedures for system owners for developing, maintaining and testing disaster recovery/contingency plans. In addition, NCUA has not developed a contingency test plan for the NCUA Accounting System (NAS) and has not completed testing of NAS for FY 2009. This issue is a repeat finding from the FY 2008 FISMA review.

NIST SP 800-53, Revision 2, guides that organizations:

- Test and/or exercise the contingency plan for the information system at least annually, using organization-defined tests or exercises to determine the plan's effectiveness and the organization's readiness to execute the plan.

- Review the contingency plan test/exercise results and initiate corrective actions.

In response to the FY 2008 FISMA review, NCUA officials agreed with our recommendation to establish policies and procedures for developing, maintaining, and testing disaster recovery and contingency plans. They agreed to complete this by

[12] In its FY 2009 Reporting Instructions, OMB indicates it does not recognize the interim authority to operate.
[13] An interim authorization provides a limited authorization to operate the information system under specific terms and conditions and acknowledges greater risk to the agency for a specified period of time.

June 1, 2009. In addition, they agreed to test and update the plans at least annually. However, NCUA officials have not developed an overall policy and procedure that provides guidance to system owners for developing, maintaining, and testing contingency plans. In addition, NCUA officials do not have a contingency plan to test NAS and did not complete FY 2009 contingency plan testing for NAS. Furthermore, while NCUA completed contingency plan testing for GSS, they could not provide the contingency plan for GSS. NCUA officials indicated they are in the process of developing the contingency plans for NAS and GSS, but they did not provide an estimated completion date.

By not developing overall policies and procedures, and routinely testing and updating its IT system disaster recovery and contingency plans, NCUA cannot ensure its ability to continue operations for information systems that support its operations and assets.

**Recommendation 15:** We recommend that NCUA:

1) Establish policies and procedures for developing, maintaining, and testing disaster recovery and contingency plans, and test and update the plans at least annually;

2) Document the contingency plan for the NCUA Accounting System (NAS) and NCUA General Support System (GSS).; and

3) Test the NAS contingency plan prior to the end of FY 2009.

***Agency Response:*** *NCUA agrees.*

*Estimated completion date for items #1 and #2: 5/1/2010*
*Estimated completion date for item #3: 12/31/2009.*

**OIG Response:** The OIG concurs with NCUA's planned actions.