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) 2010

Report # OIG-10-18
November 15, 2010

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, 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 November 8, 2010 to discuss evaluation results.

The NCUA has worked to further strengthen its information technology (IT) security program during Fiscal Year (FY) 2010. NCUA's accomplishments during this period include:

- Enhanced change control management system, adding security impact analysis for its IT systems.
- Use of an SCAP-validated scanner to verify its workstation configurations.
- Enhanced policies and procedures.
- Completed e-Authentication risk assessments for its two e-Authentication systems.
- Completed security control assessments for five of its six FISMA systems.
- Signed Authorizations To Operate for all six Certification and Accreditation packages.
- Improved Plan of Action and Milestones process.
- Updated Privacy Policy on NCUA.gov to describe use of third-party Web sites and applications.

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

- Improve its security configuration program.
- Improve its contingency planning program for its FISMA systems.
- Enhance its procedures for ensuring terminated users and inactive user accounts are removed from its systems.
- Update the Service Level Agreement for its Intrusion Detection System.
- Implement continuing education requirements for its information technology employees.

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

- Perform a security control assessment for its General Support System.
- Complete an overall Business Impact Assessment of its FISMA systems.
- Improve its oversight of external service providers.
- Improve its remote access controls.
- Improve its Plan of Action and Milestone process.
- Review its use of Personally Identifiable Information and Social Security Numbers.

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 2010 Reporting Instructions for the Federal Information Security Management Act on April 21, 2010. 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 and 2 board members. 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 FISCAM, NIST SPs, and 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 the POA&M process, privacy and security awareness training, remote access, identity management program, continuous monitoring, and incident response. In addition, we evaluated areas required to report under OMB M-10-15, 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 August 2010 through November 2010. 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. NCUA verifies FDCC security configurations for its workstations using FDCC scanner capabilities and has documented its compliance with/variances from NIST baseline security configurations for its workstations. However, NCUA has not implemented the NIST-approved security configurations for its servers and network devices. In addition, NCUA has not implemented a procedure and tool to verify its server and network device configurations against the NIST baseline security configurations.

The server and network device finding remains from the FY 2009 FISMA review.

FISMA requires each agency to determine minimally acceptable system configuration requirements and ensure compliance with them.[1] 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 (NCP)[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 National Checklist Program (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 has not implemented the applicable NIST security checklists provided under the NCP to configure its servers and network devices. Concerning the servers, NCUA uses the Microsoft Baseline Security Analyzer (MBSA) to provide a baseline security configuration and verify the configurations of its servers. However, 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 has not implemented a SCAP scanner with Authenticated Configuration Scanner capabilities to ensure compliance of the network devices with the baseline configurations.

In response to the FY 2009 Independent FISMA Evaluation Report, NCUA management concurred with this finding. However, management indicated they did not implement our recommendations by their stated goal of May 2010 due to IT staff resource constraints and additional security priorities taking precedence.

By not adopting the NIST-approved server security configuration checklist, the 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 servers, and network devices (e.g., routers, switches, firewalls etc).

Recommendation 1: We recommend that NCUA take the following actions:

1) Implement a Security Content Automation Protocol (SCAP) validated vulnerability scanner/appliance with Authenticated Configuration Scanner capabilities for servers and network devices.

2) 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, but notes that this finding has no impact on the actual security of NCUA systems. We are currently using a scanning tool that executes the required scan, but does not present the information in the SCAP format. We will review SCAP validated tools in order to determine if the extra functionality is cost justified.*

[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.

OIG Response: The OIG re-emphasizes that NCUA's use of non-SCAP validated tools results in NCUA not meeting OMB requirements. More importantly, the use of SCAP validated tools in combination with the National Checklist Program would facilitate NCUA mapping its individual system security configuration settings to the high-level security requirements as identified by NIST.

2. NCUA needs to perform a security control assessment for its General Support System.

NCUA did not assess the management, operational, and technical security controls for its General Support System (GSS) in FY 2010.

NIST SP 800-37 states that periodic testing and evaluation of the effectiveness of information security policies, procedures, practices, and security controls to be performed with a frequency depending on risk, but no less than annually.

NIST SP 800-53A, Revision 1, describes the process of assessing the security controls in organizational information systems including: (i) the activities carried out by organizations and assessors to prepare for security control assessments; (ii) the development of security assessment plans; (iii) the conduct of security control assessments and the analysis, documentation, and reporting of assessment results; and (iv) post-assessment report analysis and follow-on activities carried out by organizations.

NCUA officials indicated they did not assess the GSS this year because they were under the impression that the System Test and Evaluation from the FY 2009 Certification &Accreditation (C&A) was still valid.

Security threats and vulnerabilities to IT systems change continuously. By maintaining comprehensive C&A packages for all systems including ongoing security control assessments, NCUA will be able to identify all of the security vulnerabilities associated with operating their system. Consequently, NCUA management actions on this issue will be able to help maintain the confidentiality, availability, and integrity of data in the GSS.

Recommendation 2: Conduct a security control assessment for the GSS according to NIST guidance.

Agency Response: *NCUA agrees with the recommendations and has scheduled a test of the GSS controls with KPMG that will be completed in the next FISMA calendar cycle.*

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

3. NCUA needs to complete an overall Business Impact Analysis of its FISMA systems.

NCUA has not completed an overall Business Impact Analysis of its systems that are critical to supporting the organization's mission/business functions.

NIST 800-34, Revision 1, provides the following guidance:

Effective contingency planning begins with the development of an organization contingency planning policy and subjection of each information system to a Business Impact Analysis (BIA). This facilitates prioritization of systems and processes based on the FIPS 199 impact level and develops priority recovery strategies for minimizing loss. FIPS 199 provides guidelines on determining information and information system impact to organizational operations and assets, individuals, other organizations, and the nation through a formula that examines three security objectives: confidentiality, integrity, and availability.

Performing a Business Impact Analysis includes determining business processes and recovery criticality, identifying resource requirements, and identifying system resource recovery priorities.

The BIA purpose is to correlate the system with the critical mission/business processes and services provided, and based on that information, characterize the consequences of a disruption. The Information System Contingency Plan (ISCP) Coordinator can use the BIA results to determine contingency planning requirements and priorities.

NCUA has not performed an overall Business Impact Assessment in accordance with NIST SP 800-34, Revision 1 guidance.

By not performing an overall Business Impact Assessment, it will be more difficult for NCUA to prioritize the systems and processes based on the FIPS 199 impact level and to develop priority recovery strategies for minimizing loss.

Recommendation 3: We recommend that NCUA management complete its overall Business Impact Assessment on each of its systems.

Agency Response: *NCUA agrees with the recommendation.*

OIG Response: The OIG concurs.

4. 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 provided a contingency plan for the NCUA Accounting System (NAS). This issue is a repeat finding from the FY 2008 and FY 2009 FISMA reviews.

Furthermore, NCUA has not completed testing of its NCUA systems for FY 2010.

NIST 800-53, Revision 3, guides provides the following guidance to organizations:

- Test and/or exercise the contingency plan for the information system using organization-defined tests and/or exercises on an organization-defined frequency to determine the plan's effectiveness and the organization's readiness to execute the plan; and

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

NCUA has not completed FY 2010 contingency plan testing on any of its six FISMA systems. In addition, although NCUA officials indicated they have developed a contingency plan for NAS, officials did not provide this plan for NAS. Furthermore, in response to our FY 2009 FISMA review, NCUA management agreed with our recommendation to develop policies and procedures for system owners for developing, maintaining and testing contingency plans. NCUA management indicated they would implement the recommendation by May 1, 2010. However, as of the date of this review, NCUA management had not implemented the recommendation.

NCUA management indicated there was an oversight in not establishing the policies and procedures as agreed. However, they did not indicate why they have not tested the FISMA systems this year. In addition, NCUA officials did not provide a formal contingency plan for NAS.

By developing and routinely testing its IT system disaster recovery and contingency plans or including all key elements within a documented contingency plan, NCUA can help ensure its ability to continue to operate the information systems that support its operations and assets.

Recommendation 4: We recommend that NCUA take the following actions:

1) Establish policies and procedures for developing, maintaining, and testing disaster recovery and contingency plans, as well as test and update the plans on an organization-defined frequency (to be determined).

2) Document and provide the formal contingency plan for the NCUA Accounting System; and

3) Test the NCUA contingency plans for each FISMA system according to NCUA-defined frequency.

Agency Response: *NCUA agrees with the recommendation.*

OIG Response: The OIG concurs.

5. NCUA needs to improve its oversight of external service providers.

NCUA needs to improve its process for overseeing external service providers to include contractors and government agencies.

NIST SP 800-53 Revision 3 provides the following guidance:

- Requires that providers of external information system services comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

- Defines and documents government oversight and user roles and responsibilities with regard to external information system services.

- Requires organizations to monitor security control compliance by external service providers.

We determined NCUA does not have a documented methodology for performing oversight and evaluation on contractor systems or systems hosted at other government agencies. Consequently, there was no methodology in place when NCUA implemented its new Financial Management System (Delphi) in FY 2010, operated externally by the Department of Transportation (DOT). We reviewed the NCUA/DOT Interagency Agreement for Delphi and determined it includes security language requiring compliance with FISMA. However, NCUA does not have a copy of the Authority to Operate (ATO) or security Service Level Agreements (SLAs) with DOT. In addition, NCUA did not have the oversight compliance documentation agreed to as part of the Interagency Agreement. This documentation includes monthly security status reports detailing DOT's FISMA compliance, mitigation status trends and the overall security posture of the system.

By not appropriately monitoring security control compliance by external service providers, the potential for security incidents increases which could put the overall confidentiality, integrity, and availability of sensitive data shared between NCUA and external systems at risk.

Recommendation 5: We recommend that the NCUA take the following actions:

1) Define and document policies and procedures for an oversight methodology of external information system services with contractors.

2) Monitor security control compliance by external service providers and maintain the required inventory items.

3) Maintain agreements (i.e., security Service Level Agreements, Interconnection Security Agreements, and contracts between NCUA and external service providers.

Agency Response: *NCUA agrees with the recommendations. We will create agency policy that will address these items as well as update the NCUA contracting manual in order to address security requirements with external providers.*

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

6. NCUA needs to improve its remote access controls.

According to the results of the NCUA's E-Authentication Risk Assessments, the Examiner Support System (ESS) and the Online Data Collection System (ODCS) require Level 3 Multifactor Authentication. However, these applications only implement one factor (a user name and password). In addition, NCUA only requires one-factor authentication for remote access to its network.

OMB M-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information*, requires that agencies allow remote access only with two-factor authentication where one of the factors is provided by a device separate from the computer gaining access.

NIST SP 800-63, P 11 states "Authentication systems are often categorized by the number of factors that they incorporate. The three factors often considered as the cornerstone of authentication are:

- Something you know (for example, a password)
- Something you have (for example, an ID badge or a cryptographic key)
- Something you are (for example, a voice print or other biometric)"

NIST SP 800-63, P 11, P 34 states "Level 3 authentication is based on proof of possession of a cryptographic key using a cryptographic protocol. Level 3

authentication assurance requires cryptographic strength mechanisms that protect the primary authentication token (a secret key or a private key) against compromise by the following protocol threats defined in section 8.1.1: eavesdropper, replay, on-line guessing, verifier impersonation and man-in-the-middle attacks. Level 3 also requires two factor authentication; in addition to the key, the user must employ a password or biometric to activate the key."

According to the results of the Risk Assessments, ESS and ODCS require Level 3 Multifactor Authentication. However, NCUA only uses one factor authentication (a user name and password) for access to ESS and ODCS. In addition, NCUA only uses one-factor authentication for remote access to its network. NCUA policy does not require multifactor authentication for its network and NIST 800-63 Level 3 and Level 4 systems.

By implementing OMB and NIST technical security considerations and requirements, NCUA will help protect its systems and data from the risk of unauthorized exposure. Should a breach of information occur (e.g. Financial Sector Oversight information) NCUA's reputation could be hurt and it could have a serious adverse effect on organizational operations, assets, or individuals.

Recommendation 6: We recommend that NCUA:

1) Require multifactor authentication for remote access to the NCUA network.

2) Require multifactor authentication for access to NCUA Level 3 and Level 4 e-Authentication systems.

3) Implement multifactor authentication for remote access to the NCUA network, and for access to the Examiner Support System and the Online Data Collection System.

Agency Response: *NCUA agrees with the recommendations in principle, but is prepared to accept the residual risk in using the systems as they are currently implemented. Over the years, we have spent considerable effort engineering the current access methods that address both information security as well as the connectivity needs of our remote work force.*

OIG Response: The OIG emphasizes that using multi-factor authentication as compared to the current methodology would provide NCUA with optimum protection of its systems and data and ultimately its operations. NCUA's own 'Security Policy and Procedures' document indicates that 'improved security comes by moving from the user ID/password environment…to the smart card/PIN environment….'

7. NCUA needs to improve its Plans of Action and Milestones process.

For some Plans of Action and Milestones (POA&M) items, NCUA needs to provide support that the items marked as "completed" were actually accomplished.

OMB and FISMA require agency officials to maintain sufficient POA&M evidence. Additionally, OMB and FISMA require agency officials to be involved in agency efforts to review and periodically update remediation efforts to correct outstanding weaknesses.

OMB M-04-25 states that OMB requires agencies to prepare POA&Ms for all programs and systems where an IT security weakness has been found. The guidance directs CIOs and agency program officials to develop, implement, and manage POA&Ms for all programs and systems they operate and control (e.g., for program officials this includes all systems that support their operations and assets). Additionally, program officials shall regularly (at least quarterly and at the direction of the CIO) update the agency CIO on their progress to enable the CIO to monitor agency-wide remediation efforts and provide the agency's quarterly update to OMB. M-04-25 also provides instructions on how POA&Ms should be structured and maintained.

Although NCUA's POA&M process provides supporting documentation for most POA&M items, NCUA does not provide supporting documentation for some POA&M items marked as completed. In addition, NCUA management does not sign-off each completed POA&M item as part of POA&M oversight.

NCUA officials indicated that some actions to complete POA&M items are not documentable and that the Information Security Officer visually verifies these items as the responsible party completes them. We have discussed with NCUA officials that they should certify they reviewed or observed the remediation for those POA&M items as opposed to just signing them off as "completed." In addition, NCUA officials indicated that NCUA management is not involved in signing off that items are completed.

By appropriately annotating or documenting each completed POA&M item, NCUA management can ensure that it is clear to all interested parties that NCUA has adequately addressed completed POA&M items. Ultimately, this will help reinforce NCUA's efforts to protect the confidentiality, availability, and integrity of NCUA data and systems.

Recommendation 7: We recommend that the NCUA:

1) Obtain and maintain documentation to support all completed Plan of Action and Milestone items.

2) Require the NCUA Information Security Officer to formally certify the completion of POA&M items that are not documentable, but that are visually observed as completed.

3) Require NCUA management to sign-off each completed POA&M item.

Agency Response: *NCUA agrees with the recommendations. The position of the Deputy Chief Information Officer is currently vacant, but when filled, this person will verify that each item is fully completed and documented.*

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

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

We identified active user accounts for terminated employees on some NCUA systems.

This issue is a repeat finding from the FY 2009 FISMA review.

NIST SP 800-12 indicates that 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 800-53, Revision 3, provides the following guidance:

- 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.

We reviewed NCUA's listing of terminated NCUA employees against its list of Active Directory accounts and determined that terminated employees had active user accounts on NCUA systems as follows:

- Six users on the General Support System (GSS)
- Five users on the Online Data Collection System (ODCS)
- One user on the Insurance Information System (IIS)

Last year, NCUA officials informed us they implemented a new process to review and disable inactive Active Directory user accounts on a weekly basis. However, the process only applied to a review of GSS accounts. In response to our FY 2009 FISMA review, NCUA management agreed with the OIG's recommendations, which would have addressed these issues. NCUA management estimated a completion date of December 31, 2009. However, NCUA management did not formalize/document and update its process to review and disable inactive user accounts. We believe this has

resulted in NCUA management not consistently executing the process as evidenced by the user accounts identified above that NCUA should have deactivated.

By disabling inactive user accounts and removing the access of terminated employees in a timely manner, NCUA will prevent existing and former employees from using 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 8: We recommend that NCUA:

1) Formally document its process for reviewing and disabling inactive user accounts.

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

3) Immediately review Active Directory accounts and system user accounts to identify and remove accounts for terminated employees.

Agency Response: *NCUA agrees with the recommendations. While it is reasonable to expect a handful of people to appear on this list for any given point in time, we will automate the process that generates the list and document any valid exceptions*

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

9. NCUA needs to update the Service Level Agreement for its Intrusion Detection System.

NCUA's formal Service Level Agreement (SLA) for its Intrusion Detection System (IDS) does not include requirements for specific security considerations and response times.

This issue is a repeat finding from the FY 2009 FISMA review.

NIST 800-53, Revision 3, provides the following guidance:

- Require providers of external information system services to comply with organizational information security requirements and employ appropriate security controls in accordance with applicable federal laws, Executive Orders, directives, policies, regulations, standards, and guidance.

- Define and document government oversight and user roles and responsibilities with regard to external information system services.

- Monitor security control compliance by external service providers.

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 United States Computer Emergency Readiness Team (US-CERT) requirements.

In response to the FY 2009 FISMA report, NCUA management indicated they did not formally incorporate specific security considerations and response times in the SLA because they purchased the service through a grandfathered GSA Schedule agreement. In addition, NCUA management indicated they were reviewing their current IDS service for possible replacement. NCUA management also indicated that if the service was still in place after the end of the year, they were going to establish an updated SLA with the current vendor. NCUA management gave an estimated completion date of December 31, 2009.

NCUA officials did not provide a rationale for why they did not update the existing SLA with the current vendor as they indicated. However, NCUA officials indicated they are evaluating new IDS devices and are still planning to upgrade to a new IDS service in the near future.

By establishing specific security considerations and response time requirements in the SLA that the service provider must meet, NCUA management can help ensure that it will meet the reporting requirements of OMB, NIST, FISMA, and US-CERT and enhance its ability to protect the confidentiality, availability, and integrity of NCUA data and systems.

Recommendation 9: We recommend that NCUA:

1) Update its Service Level Agreement with its Intrusion Detection System service provider to include the necessary security considerations and response time requirements (as mandated by OMB, NIST, FISMA, and US-CERT) if NCUA has not identified a replacement service provider by December 31, 2010.

2) Include the necessary security considerations and response time requirements in its Service Level Agreement with its new Intrusion Detection System service provider.

Agency Response: *NCUA agrees with the recommendations. NCUA is in the process of terminating the current IDS contract and executing intrusion detection in-house. We will implement procedures governing security parameters and response times to adequately secure the system perimeter.*

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

10. NCUA needs to review its use of Personally Identifiable Information and Social Security Numbers.

NCUA has not performed a review of its holdings of Personally Identifiable Information (PII) and Social Security Numbers (SSNs), and, if necessary, reduced its use of PII and SSNs.

OMB M-07-16 requires:

- Agencies review current holdings and reduce the volume of PII.

- Reduce the use of Social Security Numbers and eliminate any unnecessary use, and explore alternatives for a personal identifier for both Federal employees and in Federal programs.

In addition, OMB Memorandum 07-16 indicates that:

- Agency-specific implementation plans and progress updates regarding this review will be incorporated as requirements in agencies' annual reports under FISMA. Following this initial review, agencies must develop and make public a schedule by which they will periodically update the review of their holdings. This schedule may be part of an agency's annual review and any consolidated publication of minor changes of Privacy Act Systems of Records Notices (SORN).

- Within 120 days from the date of this memo, agencies must establish a plan in which the agency will eliminate the unnecessary collection and use of Social Security Numbers within eighteen months.

NCUA officials have not conducted an initial review to determine the amount of PII at NCUA, and to take steps, if necessary, to reduce the amount of PII and SSNs at NCUA.

By performing a review to determine the amount of PII and use of SSNs at NCUA, and if necessary, reducing the amount of PII and use of Social Security Numbers, NCUA will reduce the risk of exposing its sensitive data to a breach of confidentiality by an authorized or unauthorized entity.

Recommendation 10: We recommend that NCUA:

1) Review current holdings of Personally Identifiable Information and, if necessary, develop a plan to reduce any unnecessary use of PII and provide progress updates.

2) Review and if necessary, create and execute a schedule to eliminate any unnecessary collection and use of Social Security Numbers, and if applicable, explore alternatives for a personal identifier for Federal employees and in Federal programs.

Agency Response: *NCUA agrees with the recommendations. Agency staff recently received training in assessing privacy compliance aimed at inventorying and reducing PII and use of SSNs. Staff will develop a plan to obtain a baseline for this information in the coming months including a scan for PII across central data stores. Following establishment of the baseline, staff will work with offices, as necessary, to reduce any unnecessary use of PII including SSNs.*

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

11. NCUA needs to implement continuing education requirements for its information technology employees.

NCUA management has not established specialized training requirements for NCUA's information technology (IT) employees.

This is a finding from the FY 2007 FISMA evaluation, which was repeated in the FY 2008 and FY 2009 FISMA evaluation.

NIST SP 800-53, Revision 3, 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 job specific information system security training.

Additionally, 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.

NCUA management's response to this finding in the FY 2009 FISMA report was that its current policy relies on each manager's discretion to determine the security training required by employees with significant security responsibilities, which is determined each year and documented using NCUA's Individual Development Plan (IDP) process. In addition, NCUA management indicated that in order to make this process more robust, they would require a meeting of managers at the beginning of each IDP cycle to establish that year's security training requirements, which will be documented and stored with the security plan. NCUA management gave an estimated completion date of October 31, 2009.

We determined that although OCIO officials indicated they were planning to hold a meeting to accomplish security training requirements for IT employees, they have not yet established or documented these requirements.

By defining a training requirement program and requiring IT employees to take security-related training, NCUA can help ensure its IT employees have the most current technical knowledge to effectively protect the confidentiality, availability, and integrity of its sensitive data and systems.

Recommendation 11: We recommend the NCUA OCIO establish documented continuing education requirements for IT employees.

Agency Response: *NCUA agrees with the recommendation.*

OIG Response: The OIG concurs.