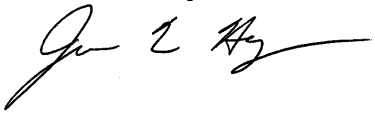
NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MANAGEMENT ACT (FISMA) 2012

Report # OIG-12-13
November 15, 2012

William A. DeSarno
Inspector General

Released by:



James Hagen
Deputy Inspector General

Auditor-in-Charge:

W. Marvin Stith, CISA
Sr. Information Technology Auditor

Table of Contents

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged Mitchell & Titus, LLP (Mitchell & Titus), to independently evaluate NCUA's 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.

Mitchell & Titus evaluated NCUA's security program through interviews, documentation reviews, technical configuration reviews, and sample testing. Mitchell & Titus evaluated NCUA against such laws, standards, and requirements as those provided through FISMA, the E-Government Act, National Institute of Standards and Technology (NIST) standards and guidelines, the Privacy Act, and Office of Management and Budget (OMB) memoranda and security and privacy policies.

While NCUA has worked to further strengthen its information security program during Fiscal Year (FY) 2012, we identified three issues remaining from last year's FISMA evaluation that NCUA officials need to address:

- Developing a Continuous Monitoring strategy and plan;
- Reviewing (and reducing) holdings of Personally Identifiable Information; and
- Addressing the minimum security controls in the Asset Management and Assistance Center Security Plan.

In addition, we identified new findings in each of the following areas and made 29 recommendations where NCUA could continue to improve its information security and privacy programs:

- Continuous Monitoring
- Risk Management
- Plan of Actions and Milestones (POA&M)
- Configuration Management
- Identity and Access Management
- Remote Access Management
- Incident Response and Reporting
- Contingency Planning
- Security Capital Planning
- Security Training
- Contractors Systems
- Privacy

We appreciate the courtesies and cooperation provided to our staff and Mitchell & Titus staff during this audit.

II. BACKGROUND

This section provides background information on the Federal Information Security Management Act (FISMA) and the National Credit Union Administration (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.

The Department of Homeland Security (DHS) issued the FY 2012 reporting metrics (February 14, 2012), which provide measures against which agency Chief Information Officers, Offices of Inspector General, and Senior Agency Officials for Privacy assess the status and compliance of agencies' information security and privacy management programs.[1] OMB issued the FY 2012 Reporting Instructions for the Federal Information Security Management Act and Agency Privacy Management on October 2, 2012. This document provides instructions to agencies for meeting its reporting requirements under FISMA. In addition, it includes instructions for reporting on agencies' privacy management programs. Furthermore, it includes clarifications to help agencies implement and meet FISMA and privacy requirements.

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

[1] DHS is exercising primary responsibility within the Executive Branch for the operational aspects of Federal agency cyber security with respect to the Federal information systems that fall within FISMA under 44 U.S.C. §3543.

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 (NCUA Board) consisting of a chairman and two members. The chairman is appointed by the President of the United States and confirmed by the Senate. No more than two board members can be from the same political party, and each member serves a staggered six-year term. The NCUA Board regularly meets in open session each month, with the exception of August, in Alexandria, Virginia.

III. OBJECTIVE

The audit objective was to assist the OIG in performing an independent evaluation of NCUA information security and privacy management 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 and privacy management programs;
- 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 the status and effectiveness of NCUA's information security and privacy management programs to enable the OIG to report to OMB.

IV. METHODOLOGY AND SCOPE

We evaluated NCUA's information security and privacy management programs and practices against such laws, standards, and requirements as those provided through FISMA, the E-Government Act, NIST standards and guidelines, the Privacy Act, and OMB memoranda and security and privacy policies.

During this audit, we assessed NCUA information security and privacy management programs in the areas identified in The Department of Homeland Security's FY 2012

Inspector General FISMA Reporting Metrics. These areas included: risk management, configuration management, incident response and reporting, security training, POA&M, remote access management, identity and access management, continuous monitoring management, contingency planning, contractor systems, and security capital planning.

We conducted our fieldwork from August 2012 through October 2012. We performed our audit in accordance with generally accepted government auditing standards. The standards require that we plan and perform the audit to obtain sufficient and appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objectives. We believe that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objectives.

V. RESULTS IN DETAIL

Information security and privacy program planning and management controls are designed to provide the framework and continuing cycle of activity for managing risk, developing security and privacy policies, assigning responsibilities, and monitoring the adequacy of information security- and privacy-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 Continuous Monitoring Program

NCUA has some automated tools (e.g., intrusion detection, Secure Content Automation Protocol), and policies and procedures that would be components of a continuous monitoring program. However, NCUA has not completely implemented a Continuous Monitoring strategy and plan. Specifically, NCUA has not documented Continuous Monitoring policies and procedures and has not fully integrated the various components of its information security program into a strategy that facilitates near real-time monitoring and risk management. This is a repeat finding from the 2011 FISMA evaluation. This finding includes issues in the following areas that we address in other sections of the report.

- Risk management policies and procedures (see page 7);
- Plans of Action and Milestones (see page 9);
- Configuration and patch management of Macintosh computers (see page 11);
- Inventory of contractor systems (see page 22); and
- Privacy (see page 23).

In FY 2011, the Administration identified Continuous Monitoring as one of three FISMA priorities.[2] In FY 2012, Continuous Monitoring is again identified as one of the three priorities having the greatest probability of success in mitigating cyber security risks to agency information systems.

NIST SP 800-53 guides that agencies should establish a continuous monitoring strategy and implement a continuous monitoring program that includes: A configuration management process for the information system and its constituent components; a determination of the security impact of changes to the information system and environment of operation; ongoing security control assessments in accordance with the organizational continuous monitoring strategy; and reporting the security state of the information system to appropriate organizational officials.

[2] The Administration's other two priorities are Trusted Internet Connection capabilities and traffic consolidation, and Homeland Security Presidential Directive (HSPD)-12, implementation for logical access control.

NIST SP 800-137, *Information Security Continuous Monitoring (ISCM) for Federal Information Systems and Organizations* (September 2011), guides that Information Security Continuous Monitoring (ISCM) supports agency risk management decisions e.g., risk response decisions, ongoing system authorization decisions, Plans of Action and Milestones (POA&M) resource and prioritization decisions, etc. It also indicates that maintaining an up-to-date view of information security risks across an organization requires the involvement of the entire agency, from senior leaders providing governance and strategic vision to individuals developing, implementing, and operating individual information systems in support of the organization's core missions and business functions.

NIST SP-800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach* (February 2010), guides that a robust continuous monitoring program requires the active involvement of information system owners and common control providers, chief information officers, senior information security officers, and authorizing officials. The monitoring program allows an organization to: track the security state of an information system on a continuous basis; and maintain the security authorization for the system over time in highly dynamic environments of operation with changing threats, vulnerabilities, technologies, and missions/business processes.

By improving and implementing a comprehensive continuous monitoring program, NCUA will be more aware of and better prepared to respond to potential threats and vulnerabilities. Ultimately, NCUA will be able to better protect the confidentiality, integrity, and availability of its systems and data.

Recommendation: We recommend that NCUA management:

1. Document and implement comprehensive continuous monitoring strategies, policies and procedures in accordance with guidance under Information Security Continuous Monitoring, the Risk Management Framework and other NIST guidance.

Agency Response:

OCIO will update procedures to further address this issue. OCIO will conduct an analysis of the Risk Management Framework and adjust policies and procedures accordingly.

Due Date: TBD

OIG Response: The OIG concurs.

2. NCUA needs to improve its Risk Management Program

NCUA continues to make progress in implementing a comprehensive risk management program. However, during FY2012, NCUA did not fully implement a risk management program compliant with FISMA requirements. We determined:

- NCUA's risk management program documentation does not include organization-wide risk management strategies from organization, information, mission or business process perspectives. Specifically, NCUA policies and procedures do not address all the areas of the NIST Risk Management Framework process as listed below:

  - Selecting Security Controls – Management does not have procedures to identify and select security controls that are specific to each system. For example:

    - ✓ NCUA did not address all of the 202 moderate baseline controls included in the 17 control families[3] it identified for its General Support System (GSS).

    - ✓ NCUA's Asset Management and Assistance Center (AMAC) security plan did not address each of the minimum security controls applicable to the system's security categorization and did not match the control families identified in NIST SP 800-53. This is a repeat finding from the FY 2011 FISMA evaluation.

  - Assessing Security Controls – NCUA does not have procedures on how it will test security controls. Specifically, out of the 17 control families required by NCUA, NCUA only tested 10 control families for the GSS. In addition, each control family did not include all the controls from NIST SP 800-53 as indicated above. As a result, NCUA did not test all the controls within the 10 control families.

  - Monitoring Security Controls – NCUA does not have adequate procedures to monitor security controls specific to the NCUA environment.

- NCUA did not complete the annual testing of security controls for all the agency's systems.

- NCUA does not perform or explicitly consider security impact analyses of the GSS and the Insurance Information System (IIS) prior to implementation of configuration changes.

[3] NIST SP 800-53 identifies 18 control families. Seventeen of the control families align with the minimum security requirements for federal information and information systems as described in FIPS 200, *Minimum Security Requirements for Federal Information and Information Systems* (March 2006). The remaining control family provides controls for information security programs.

- NCUA is operating four of its five FISMA systems - the IIS; AMAC; Examination Support System (ESS); and Online Data Collection System (ODCS) - without the required Authority to Operate (ATO). The ATOs for these systems expired in 2012:

- NCUA does not have a formal mechanism in place to report the status of information security to senior management.

The Risk Management Framework - as prescribed by NIST SP 800-37 - is the foundation for implementing and maintaining an effective information security program. NIST SP 800-37 provides guidelines for applying the Risk Management Framework to federal information systems to include conducting the activities of security categorization, security control selection and implementation, security control assessment, information system authorization, and security control monitoring.

FIPS PUB 200, Minimum Security Requirements for Federal Information and Information Systems (March 2006), requires agencies to: periodically assess the security controls in organizational information systems to determine if the controls are effective in their application; develop and implement plans of action designed to correct deficiencies and reduce or eliminate vulnerabilities in organizational information systems; authorize the operation of organizational information systems and any associated information system connections; and monitor information system security controls on an ongoing basis to ensure the continued effectiveness of the controls.

NCUA does not have sufficient dedicated information security resources to monitor federal guidance on a periodic basis and maintain its procedures in compliance with that guidance or to perform security authorization functions separate from system owners.

In response to the FY 2011 FISMA evaluation, NCUA indicated it was going to: (1) work with AMAC to update the security plan; and (2) consolidate of all its systems as appendices into one system security plan under the General Support System. NCUA has been planning since last year to consolidate its five FISMA systems under its General Support System (GSS) via the security authorization process. NCUA planned to complete the security authorization by July 2012; however, due to key information technology staff changes, the security authorization was delayed and is currently in process. Completing the security authorization should address NCUA's Authority to Operate its system(s) and the issues with the AMAC security plan, which would be consolidated under the GSS security plan.

With updated and approved program policies and procedures to support its Risk Management program, NCUA will be able to better manage its information systems-related risks consistent with the Risk Management Framework. In addition, by ensuring its systems are operating with a valid ATO, coupled with a comprehensive annual control testing program, and a complete and comprehensive POA&M tracking program, NCUA could avoid or mitigate system issues that could adversely impact NCUA operations. Furthermore, by performing security impact analysis of system

configuration changes, NCUA could mitigate the chance of introducing configuration changes that could adversely impact the confidentiality, integrity and availability of its systems. Finally, adequate segregation of duties in the system security authorization process would help mitigate intentional, inadvertent or missed threats to information systems security within the NCUA systems environment.

Recommendations: We recommend that NCUA management:

2. Review its risk management program documentation and update policies and procedures based on the prescribed risk management strategies outlined within NIST guidance.

3. Schedule and complete the system security authorization process on a timely basis such that all agency systems are continuously operating under a valid approved Authority to Operate.

4. Document, implement, and annually test all controls for its systems as identified in NIST guidance.

5. Implement and monitor the timely completion of annual security testing.

Agency Response:

OCIO is currently executing an independent certification and accreditation process which covers the entire new consolidated NCUA GSS. This process will address all issues listed here including updates to the documentation necessary to support future risk management actions.

Due Date: 7/29/2013

OIG Response: The OIG concurs.

3. NCUA needs to improve its Plan of Action and Milestones (POA&M) Process

While NCUA has an active POA&M process in place, we determined that NCUA policies and procedures do not provide adequate guidance in regards to how NCUA should manage its POA&M process. Specifically, NCUA has not defined the thresholds for the findings that should be added to the POA&M process and how findings outside of the POA&M process are tracked and remediated. In addition, NCUA does not have procedures to: prioritize POA&M items; track the POA&M items within the SharePoint system; define the level of effort to close POA&M items; and define the timeframe for updating and escalating the POA&M process to management.

NIST SP 800-53 guides that organizations: develop POA&Ms for the information system to document the organization's planned remedial actions to correct weaknesses

or deficiencies noted during the assessment of the security controls and to reduce or eliminate known vulnerabilities in the system; and update existing POA&Ms based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities. In addition, a dedicated information security resource is critical to ensuring that the CIO, Deputy CIO, system owners and other key NCUA staff are continually updated and aware of information security requirements, the risk posture of NCUA systems, and the status of mitigation plans.

NCUA does not have a dedicated resource to enhance or update POA&M policies and procedures or to manage the tasks associated with the POA&M process.

By enhancing its POA&M policies and procedures and dedicating an independent information security resource to manage the POA&M process, NCUA can correct information security weaknesses and deficiencies in a more adequate and timely manner. These enhancements would effectively improve the overall security of its information systems environment and better protect NCUA systems and data.

Recommendations: We recommend that NCUA management:

6. Enhance its POA&M policies and procedures.

7. Dedicate an independent information security resource to manage the POA&M process.

Agency Response:

OCIO will enhance procedures to refine the POA&M process to address the specific issues listed above. We would like to note one exception here. Findings outside the POA&M process will continue to be addressed on a case-by-case basis.

OCIO is currently going through reorganization and has designated a dedicated position for the Information Security Officer.

Due Date: 7/29/2013

OIG Response: The OIG concurs.

4. NCUA needs to improve its Configuration Management Program

While NCUA has made improvements in its security configuration program in recent years, NCUA does not have adequate configuration management policies and procedures: Specifically:

- NCUA's configuration management policies and procedures do not adequately address: purpose, scope, roles and responsibilities; management commitment; coordination among organizational entities necessary to control and manage configurations; and the timely processing of remediated configurations.

- NCUA has not documented the configuration baselines for the following non-Windows environments: UNIX, database management systems, and web servers. In addition, NCUA does not have an automated process to maintain baseline configuration compliance for their environment on a continuous basis.

- NCUA does not have a configuration baseline for its Macintosh computers and does not have a process in place to monitor and update critical security patches for Macintosh computers.

NIST SP 800-53, Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations* (August 2010 with updates as of May 1, 2010), guides that organizations should develop, disseminate, and review/update: a formal, documented configuration management policy that addresses purpose, scope, roles, responsibilities, management commitment, coordination among organizational entities, and compliance; and formal, documented procedures to facilitate the implementation of the configuration management policy and associated configuration management controls.

FIPS PUB 200 requires agencies to: establish and maintain baseline configurations and inventories of organizational information systems (including hardware, software, firmware, and documentation) throughout the respective system development life cycles; and establish and enforce security configuration settings for information technology products employed in organizational information systems. FIPS PUB 200 also requires agencies to: identify, report, and correct information and information system flaws in a timely manner; provide protection from malicious code at appropriate locations within organizational information systems; and monitor information system security alerts and advisories and take appropriate actions in response."

NCUA does not have dedicated information security resources to adequately document policies and procedures and to establish a comprehensive program that covers all of the systems and devices within the NCUA environment. In addition, NCUA's information systems office (the OCIO) is not responsible for managing or controlling the UNIX environment at AMAC. A contractor operates and manages AMAC's UNIX environment under AMAC's purview.

By documenting and establishing a comprehensive configuration management program, NCUA can more effectively and efficiently monitor, manage, and patch the security configurations for all systems and devices within the NCUA information system environment. Ultimately, a more comprehensive program will help ensure NCUA protects the confidentiality, integrity and availability of all the agency's systems and data.

Recommendations: We recommend that NCUA management**:**

8. Establish a comprehensive configuration management program that includes policy and procedures for monitoring, managing, and patching security configurations for all systems and devices:

9. Provide dedicated information security resources responsible for implementing, managing and overseeing NCUA's configuration management program.

10. Review and determine whether it would be in the best interest of NCUA's overall information security posture to transfer responsibility for the UNIX environment from AMAC to the OCIO.

Agency Response:

OCIO will conduct an analysis of the current configuration management program in light of the new NIST guidance. The new ISO will be responsible for management and oversight of this program.

OCIO will work with the OED to address managing AMAC operations to ensure a proper security posture.

Due Date: TBD

OIG Response: The OIG concurs.

5. NCUA needs to improve its Identity and Access Management Controls

We determined NCUA's access management policies and procedures are not in compliance with NIST guidelines and have not been updated to reflect NCUA's current procedures. Specifically:

- NCUA's process for providing access to new hires is not adequate. NCUA's user access documentation does not always include the specific level of access requested for the user or clearly indicate who approved the user access request.

- NCUA does not have an effective process to ensure the access of terminated employees and contractors has been adequately documented or removed in a timely manner. For example, we determined that:

    - Termination emails did not specify what accounts and permissions beyond the network account were to be terminated.

    - Seven of eight terminated users still had their Active Directory accounts enabled for 33 to 37 days after termination.

    - One enabled user account identified within the daily exception report, was for a September 2012 new hire that ultimately did not accept the job at NCUA. NCUA did not follow the termination process to remove the user's account.

- NCUA does not have an effective process to ensure inactive accounts are disabled in a timely manner. We reviewed NCUA user accounts for current employees, contractors, and developers; and temporary user accounts and determined there were seven accounts that had not logged into the Active Directory (AD) network for over 30 days. NCUA should have disabled these accounts.

NIST SP 800-53 guides that organizations should manage information system accounts to include: granting access to the system based on, a valid access authorization, intended system usage; and other attributes as required by the organization or associated missions/business functions; identifying account types; identifying authorized users of the information system and specifying access privileges; requiring appropriate approvals for requests to establish accounts; establishing, activating, modifying, disabling, and removing accounts; specifically authorizing and monitoring the use of guest/anonymous and temporary accounts; notifying account managers when temporary accounts are no longer required and when information system users are terminated, transferred, or information system usage or need-to know/need-to-share changes; and deactivating (i) temporary accounts that are no longer required; and (ii) accounts of terminated or transferred users.

NCUA's General Support System (GSS) System Security Plan (SSP) indicates that:

- AD account administrators will configure the Group Policy Object (GPO) to automatically terminate temporary or emergency accounts 30 days after creation.

- AD account administrators will configure the GPO to disable accounts after 30 days of inactivity unless the requesting manager specifies in writing a longer period due to business needs.

- All accounts must be deleted after 180 days of inactivity; however, the AD account administrator may disable rather than delete an inactive account upon written approval of a user's manager.

For operational reasons, NCUA no longer configures the GPO to automatically terminate or disable accounts; the process is accomplished manually. However, NCUA does not have dedicated information security resources to monitor and take action on applicable accounts in a timely manner. In addition, NCUA does not have a dedicated information security resource to update NCUA polices to reflect current NIST guidance.

By implementing current and effective logical identity and access control policies and procedures, NCUA management can help ensure access to the NCUA network and information systems is restricted to only authorized individuals. Ultimately, it will help NCUA protect the confidentiality and integrity of sensitive and confidential information.

Recommendations: We recommend that NCUA management:

11. Develop, document and implement identity and access management policies and procedures consistent with NIST guidelines. The policies and procedures should address providing, terminating, and disabling user access, and reviewing user access listings and levels on a periodic basis.

12. Update NCUA policies to reflect current procedures for monitoring and managing Active Directory user accounts.

13. Designate dedicated information security resources to update and maintain NCUA's policies and procedures in accordance with NIST guidance; and to monitor and enforce compliance with user account management policies.

Agency Response:

OCIO will update access management policies and procedures, train staff and conduct periodic reviews. OCIO will also document current procedures for monitoring active directory user accounts. The new dedicated ISO will be responsible for maintaining policies and procedures as well as monitoring compliance.

Due Date: 7/29/2013

OIG Response: The OIG concurs.

6. NCUA needs to improve Remote Access Controls

NCUA has not fully implemented adequate security controls over remote access to the NCUA network. Specifically:

- NCUA recently implemented two-factor authentication via HSPD-12 PIV authentication for all employees. However, NCUA does not provide contractors with or require contractors to use two-factor authentication to access the NCUA remotely. In addition, NCUA does not yet have a plan of action to address this risk.

- NCUA does not have an adequate process to monitor VPN accounts. We reviewed the VPN accounts that include federal employees, contractors, developers, and users with temporary access and noted that there are seven accounts that NCUA should have disabled for not logging into the network for over 30 days.

OMB M-07-16 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. Also, NCUA's General Support System (GSS) System Security Plan (SSP) indicates that Active Directory account administrators will configure the GPO to disable accounts after 30 days of inactivity unless the requesting manager specifies in writing a longer period due to business needs.

NCUA delayed the implementation of HSPD-12 PIV authentication due to key information technology personnel changes. For operational reasons, NCUA no longer configures the GPO to automatically terminate or disable accounts; the process is accomplished manually. However, NCUA does not have dedicated information security resources to monitor and take action on applicable VPN accounts in a timely manner.

By implementing strong remote access controls, NCUA would help protect its systems and data from the risk of unauthorized access remotely. In addition, by adequately monitoring VPN account activity, NCUA could prevent the use of inactive accounts by malicious individuals to exploit its network and confidential data.

Recommendations: We recommend that NCUA management:

14. Develop and document a process to implement two-factor authentication of contractors accessing the NCUA network remotely.

15. Update NCUA policies to reflect current procedures for monitoring and managing Active Directory user accounts.

16. Designate dedicated information security resources to monitor and enforce compliance with remote access account management policies.

Agency Response:

OCIO will update active directory policies and procedures to reflect current practices. OCIO will work with the OED to facilitate collaboration with OHR and OCFO to implement two factor authentications for contractor access to the network. This is an on-boarding issue that will require cooperation from all three offices. The new

dedicated ISO will be responsible for maintaining policies and procedures as well as monitoring compliance.

Due Date: TBD

OIG Response: The OIG concurs.

7. NCUA needs to improve its Incident Response and Reporting Process

While NCUA has a formal incident response and reporting process, we determined:

- Current policies and procedures do not provide guidance with regard to classifying incidents by severity levels.

- NCUA does not have a process for correlating incidents to perform trend analysis.

- NCUA does not monitor and close potential incidents in a timely manner.

NIST SP 800-61, Revision 1, *Computer Security Incident Handling Guide* (March 2008),[4] requires agencies to establish incident response capabilities, which includes requiring and providing guidance for detecting, analyzing and resolving incidents in a timely manner based on the nature and impact of the incidents. It also guides that most incident response policies include key elements, such as prioritization or severity ratings of incidents. In addition, NIST SP 800-53 guides that the organization should correlate incident information and individual incident responses to achieve an organization-wide perspective on incident awareness and response. Regarding event correlation, NIST SP 800-61 explains that: *Evidence of an incident may be captured in several logs that each contains different types of data - a firewall log may have the source IP address that was used, whereas an application log may contain a username. A network intrusion detection prevention system may detect that an attack was launched against a particular host, but it may not know if the attack was successful. The analyst may need to examine the host's logs to determine that information. Correlating events among multiple indicator sources can be invaluable in validating whether a particular incident occurred.*

NCUA does not have dedicated information security resources to adequately monitor NIST guidance to ensure agency policies and procedures are current with that guidance.

By improving its incident response and reporting process, NCUA would be able to more effectively identify, assess and resolve potential and actual security incidents. Ultimately, an improved process would help NCUA protect the confidentiality, integrity, and availability of its network, information systems and data.

[4] NIST recently issued Revision 2 of this guidance in August 2012.

Recommendations: We recommend that NCUA management**:**

17. Update its incident response and reporting policies and procedures to define and prioritize security incidents by severity levels.

18. Establish a process to monitor and close potential security incidents in a timely manner.

19. Establish a process to correlate incidents from multiple sources to perform trend analysis.

20. Designate dedicated information security resources to monitor federal guidelines and maintain agency policies and procedures in accordance with those guidelines.

Agency Response:

OCIO will update incident response policies and procedures, train staff and conduct periodic reviews. OCIO will review the process used by technical support staff in logging and tracking potential incidents. The new dedicated ISO will be responsible for maintaining policies and procedures as well as monitoring compliance.

OCIO has no plans for correlating incidents to perform trend analysis.

Due Date: 7/29/2013

OIG Response: The OIG concurs with NCUA's response regarding its incident response policies and procedures in general. However, the OIG does not concur with the agency's acceptance of the potential risk(s) associated with not correlating incidents. The OIG reiterates the significance and benefits of correlating potential incidents by highlighting guidance included in the recently revised NIST 800-61, Revision 2 (August 2012), which indicates:

> *In an organization, millions of possible signs of incidents may occur each day, recorded mainly by logging and computer security software. Automation is needed to perform an initial analysis of the data and select events of interest for human review. Event correlation software can be of great value in automating the analysis process.*

8. NCUA needs to improve its Contingency Planning process

We determined:

- NCUA's Contingency Plan for its Asset Management Assistance Center (AMAC) system is outdated. This is a repeat finding from the FY 2011 FISMA evaluation.

- NCUA has not documented and implemented preventive controls, planned maintenance, or strategies for its Insurance Information System (IIS).

- The results of the IIS Contingency Plan test do not provide an after action report or evidence of corrective actions taken.

- NCUA does not have approval letters for its General Support System (GSS) and IIS Contingency Plans to validate that the Plan documentation is complete.

FIPS PUB 200 requires agencies to establish, maintain, and effectively implement plans for emergency response, backup operations, and post-disaster recovery for organizational information systems to ensure the availability of critical information resources and continuity of operations in emergency situations.

NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010), guides that in order for an agency to develop and maintain an effective information system contingency plan, the process must include the following seven steps that represent key elements in a comprehensive information system contingency planning capability:

- Developing the policy;

- Conducting the business impact analysis;

- Identifying preventive controls;

- Creating contingency strategies;

- Developing a contingency plan;

- Ensuring plan testing, training, and exercises; and

- Ensuring plan maintenance

NIST SP 800-53 guides that the organization should revise its contingency plans to address: changes to the organization, information system, or operational environment; and problems encountered during plan implementation, execution, and testing. NIST SP 800-53 also guides that a designated official should review and approve the organization's contingency plans.

NCUA has been planning to consolidate its five systems into one overall system under its General Support System (GSS) since last year via its security authorization process. NCUA planned to complete the security authorization by July 2012; however, due to key information technology management changes, the security authorization was delayed

and is currently in process. Completing the security authorization should remediate the issues under this finding.

By implementing complete, comprehensive and current contingency planning, NCUA will have better assurance that its mission-critical system(s) will be able to continue to operate in an emergency situation whether that involves restoring data or relocating to an alternate processing site.

Recommendations: We recommend that NCUA management**:**

21. Ensure that NCUA's contingency planning process and its consolidated Contingency Plan include the following missing components:

    - A plan approval letter to validate that the Contingency Plan documentation is complete.

    - Documented and implemented preventive controls, planned maintenance, and strategies.

22. Ensure that NCUA documents evidence of corrective actions taken or an after action report as a result of Contingency Plan testing.

Agency Response:

Most of the issues will be resolved by the current C&A effort. OCIO will work with OED to resolve issue related to AMAC operations.

Due Date: TBD

OIG Response: The OIG concurs.

9. NCUA needs to improve its Security Capital Planning and Investment Program

We determined NCUA's agency wide Information Security Procedures do not adequately address a structured process to evaluate security-related needs and perform budgeting at a sufficiently detailed level. Specifically, NCUA does not have specific guidelines for planning, budgeting, and mapping major capital information technology security resource expenditures according to POA&Ms and other information technology-related initiatives. For example, we reviewed the POA&M for records related to NCUA's General Support System (GSS) and its Insurance Information System (IIS) to assess whether NCUA coordinates its budgeting activities for information technology security expenses with its POA&M remediation expenses. We found that NCUA's annual budget did not include distinct line items traceable to the agency's POA&M entries.

NIST SP 800-53 guides that organizations: include a determination of information security requirements for the information system in their mission/business process planning; determine, document, and allocate the resources required to protect the information system as part of its capital planning and investment control process; and establish a discrete line item for information security in organizational programming and budgeting documentation. In addition, NIST SP 800-53 guides that organizations should ensure that all capital planning and investment requests include the resources needed to implement the information security program and document all exceptions to this requirement.

By implementing a comprehensive Capital Planning and Investment Control process, NCUA would help ensure the agency adequately budgets its funding needs for all of its information technology security expenses. This process would help NCUA more efficiently mitigate risks and vulnerabilities within NCUA's information technology environment, ultimately helping to protect the confidentiality, integrity, and availability of NCUA's systems and data.

Recommendations: We recommend that NCUA management**:**

23. Implement Capital Planning and Investment Control procedures and guidelines to consistently and systematically drive the evaluation and documentation of security-related resources in the capital planning process. The guidance should include documentation requirements with respect to budgeting for all information security program expenses that would normally occur. These would include such expenses as the cyclical security authorization process, risk identification and mitigation activities, remediation of security weaknesses, and activities associated with day-to-day information security operations.

24. Implement a process to periodically monitor information technology security-related expenses against the budget for each information technology security component.

Agency Response:

OCIO is in the process of developing an IT prioritization council that will factor information security costs and required resources as part of the budgeting process. However, OCIO has not requested specific funding for information security in the past. OCIO will work with OED on budgeting for information security matters.

Due Date: TBD.

OIG Response: The OIG concurs.

10. NCUA needs to improve its Security Awareness Training Program

We determined NCUA procedures for Security Awareness Training (SAT) and role-based training do not reflect current NIST guidance. Specifically, NCUA does not have documented procedures for reviewing the timely completion of security awareness training by new hires. In addition, NCUA has not established a specific timeframe within which new hires must complete the agency's rules of behavior, or sanctions for new hires who do not complete the rules of behavior. Furthermore, NCUA: (1) does not have a formal and documented process to identify all roles that need specialized security training; and (2) does not specify the types and the frequency of the specialized training, or the personnel required to attend the training.

NIST SP 800-53 guides that organizations should provide basic security awareness training to all information system users (including managers, senior executives, and contractors) as part of initial training for new users, when required by system changes, and periodically thereafter. In addition, NIST SP 800-16, *Information Technology Security Training Requirements: A Role- and Performance-Based Model* (April 1998), requires training: for current employees; new employees within 60 days of hire; whenever there is a significant change in the agency's IT security environment or procedures, or when an employee enters a new position which deals with sensitive information; and periodically as refresher training, based on the sensitivity of the information the employee handles. NIST SP 800-53 also guides that organizations provide role-based security-related training before authorizing access to a system or performing assigned duties; when required by system changes; and periodically thereafter.

NCUA does not have dedicated information security resources to develop, document, implement and monitor a robust security awareness training program that meets NIST guidance and requirements.

By implementing a current and effective security awareness training program, NCUA management can help ensure all personnel receive the required security training. This includes role-based training for individuals with system security responsibilities such as system administrators, system owners and individuals that play a critical role in the administration of information security at NCUA. Individuals who receive adequate and current security training and who are aware of their security responsibilities will be better prepared to perform their assigned duties in the most secure manner. Ultimately, this helps NCUA protect the confidentially, availability, and integrity of its systems and data.

Recommendations: We recommend that NCUA management**:**

25. Designate dedicated information security resources to:

- Update the general security awareness training program and role-based training program to meet NIST guidance and requirements.

- Monitor and track the timely completion of new hire security awareness training and establish and enforce sanctions for non-compliance.

- Periodically review and update the list of individuals that need role-based training; specify frequency of role-based training; and enforce timely completion of role-based training.

Agency Response:

OCIO will continue to improve security awareness policies and procedures to be consistent with NIST guidelines. OCIO will assign a backup to ensure that the daily report for new hire security awareness training is run and enforced. OCIO will complete this year's role-based security training.

Due Date: 7/29/2013

OIG Response: The OIG concurs.

11. NCUA needs to improve Oversight of its Contractor Systems

While NCUA has a current inventory of contractor systems operating in or connected to the NCUA environment, NCUA has not fully implemented a formal contractor oversight management process in alignment with the applicable federal guidelines. Specifically:

- Current NCUA policies and procedures do not provide sufficient guidance in regards to how NCUA should monitor and assess information security requirements for its contractor systems. For example:

    - NCUA does not have a formal process in place for maintaining sufficient assurance that security controls of contractor provided or hosted systems and services - such as the GSA-PIV (Personal Identity Verification) and the Angel Parature systems - are effectively implemented and comply with federal and NCUA guidelines.

    - NCUA does not have a process in place to ensure it obtains the System Security Plans (SSPs) of contractor systems. Specifically, NCUA does not have the SSPs for two of its three contractor systems - the Angel Parature or the GSA PIV systems.

    - NCUA does not have a formal process for capturing and maintaining an inventory of contractor systems under FISMA inventory requirements.

- NCUA does not have a Memorandum of Understanding or Interconnection Security Agreement (MOU/ISA) for the Angel Parature system.

NIST SP 800-53 guides that organizations develop and maintain an inventory of its information systems. In addition, NIST SP 800-53 guides that organizations: authorize connections from their information systems to other information systems outside of the authorization boundary through the use of Interconnection Security Agreements, and document - for each connection - the interface characteristics, security requirements and the nature of the information communicated; and monitor the interconnections on an ongoing basis to verify enforcement of security requirements.

While OCIO is centrally responsible for the security of all systems operating in the NCUA environment, functional system owners are responsible for obtaining and maintaining system security documentation for their contractor systems without oversight from or the involvement of OCIO.

By improving its contractor oversight process, NCUA can have better assurance that contractor systems operating in or connected to the NCUA systems environment have the same information security measures implemented as NCUA's systems. As a result, NCUA could better ensure that threats to its network are protected against compromise and better ensure the confidentiality and integrity of NCUA data.

Recommendations: We recommend that NCUA management:

26. Develop and implement a formal process to centrally monitor and maintain an inventory of contractor systems and obtain from system owners the associated approved security documentation (e.g., System Security Plans, Interconnection Security Agreements, etc.) in accordance with NIST guidance.

Agency Response:

OCIO will improve policies and procedures to monitor security of contractor systems. OCIO will work with system owners to maintain appropriate security documents in accordance with NIST guidance.

OCIO would like to make one observation. It is not always possible to obtain security plans for contractor systems. In lieu of a security plan we gather SAE16 documents and Accreditation letters.

Due Date: 7/29/2013

OIG Response: The OIG concurs.

12. NCUA needs to improve its Privacy Program

NCUA has not completed an initial review of its holdings of Personally Identifiable Information (PII), and if necessary, reduced its use of PII and Social Security Numbers (SSNs). This is a repeat finding from the FY 2011 FISMA evaluation. In addition,

NCUA has not done an assessment to determine whether it needs to conduct a Privacy Impact Analysis (PIA) for its systems and has not developed a privacy program to monitor its use and handling of PII on a continuing basis.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010), indicates that organizations: are required to identify all PII residing within their organization or under the control of their organization through a third party; and should minimize the use, collection, and retention of PII to what is strictly necessary to accomplish their business purpose and mission. It also reiterates that OMB Memorandum-07-16, *Safeguarding Against and Responding to the Breach of Personally Identifiable Information* (May 22, 2007), required that agencies:

- Review current holdings of PII and ensure they are accurate, relevant, timely, and complete;
- Reduce PII holdings to the minimum necessary for proper performance of agency functions;
- Develop a schedule for periodic review of PII holdings; and
- Establish a plan to eliminate the unnecessary collection and use of SSNs.

OMB Memorandum-03-22, *OMB Guidance for Implementing the Privacy Provisions of the E-Government Act of 2002* (September 26, 2003), indicates that in addition to the requirements identified in the E-Government Act, agencies must in general perform and update a PIA as necessary where a system change creates new privacy risks.

NIST SP 800-122 guides that organizations often use a Privacy Threshold Analysis (PTA) to determine if a system contains PII, whether a PIA is required, whether a System of Records Notice (SORN) is required, and if any other privacy requirements apply to the information system.[5] It adds that PTAs are useful in initiating the communication and collaboration for each system between the privacy officer, the information security officer, and the information officer.

Organizational and staff changes surrounding oversight of the privacy program delayed NCUA in completing its initial review of PII. In addition, NCUA was not aware that it needed to conduct a PIA on its existing systems.

By performing a review to determine the amount of PII the agency holds and conducting a PTA (or PIA) for its systems, NCUA will mitigate the risk of exposing its sensitive data to a breach of confidentiality by an authorized or unauthorized entity. Ultimately, this could prevent public embarrassment for the agency and a loss of trust by the public.

[5] Other examples of methods to identify PII include reviewing system documentation, conducting interviews, conducting data calls, using data loss prevention technologies (e.g., automated PII network monitoring tools), or checking with system and data owners.

Recommendations: We recommend that NCUA management:

27. Complete an initial review of NCUA's current holdings of Personally Identifiable Information (PII) and, if necessary, develop a plan to reduce any unnecessary use of PII.

28. Assess whether NCUA's system(s) require a PIA in the near term.

29. Develop a privacy program that includes policies and procedures for monitoring the usage and handling of PII on a continuous basis, determining when to perform a PIA, and the process for completing a PIA.

Agency Response:

The Office of General Counsel agrees with the recommendations and the Senior Agency Official for Privacy (SAOP) has initiated responsive actions. For example, in conjunction with NCUA's IT Systems Inventory Initiative, we are collecting information identifying systems containing PII and whether a PIA is required. We also are coordinating with the Office of the Chief Information Officer to identify planned system changes or procurements that will require a PIA. Additionally, as part of a comprehensive review of NCUA's privacy program, NCUA will review and revise as necessary its general privacy instruction and individual offices' policies and procedures to address the usage and handling of PII. We will also continue ongoing privacy awareness training efforts including an expansion of targeted training for individual offices.

OIG Response: The OIG concurs.