NATIONAL CREDIT UNION ADMINISTRATION
OFFICE OF INSPECTOR GENERAL

FY 2016
INDEPENDENT EVALUATION OF THE NATIONAL CREDIT UNION ADMINISTRATION'S COMPLIANCE WITH THE FEDERAL INFORMATION SECURITY MODERNIZATION ACT OF 2014

REPORT # OIG-16-08
NOVEMBER 10, 2016

James W. Hagen
Inspector General

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY

The Office of Inspector General (OIG) for the National Credit Union Administration (NCUA) engaged CliftonLarsonAllen LLP (CLA) to independently evaluate NCUA's information systems and information security program and controls for compliance with the Federal Information Security Modernization Act of 2014 (FISMA 2014).

CLA evaluated NCUA's information security and privacy management programs through interviews, documentation reviews, technical configuration reviews, and sample testing. CLA 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 privacy and information security policies.

In addressing and resolving prior year issues and recommendations, NCUA has continued to strengthen its information security program during Fiscal Year (FY) 2016.

Regarding its prior year findings:

- NCUA has made significant progress towards furthering its privacy program. Management indicates it is on track to finalize its program by December 31, 2016, as indicated in response to the 2015 FISMA report.

- NCUA has made significant progress towards addressing its risk management program. Management indicates it is on track to complete defining and communicating its organization-wide risk tolerance by December 31, 2016, as indicated in response to the 2015 FISMA report.

- NCUA has one partial finding remaining from last year pertaining to one unsupported software component that management indicates the agency will address by June 30, 2016.

With new staffing, NCUA's Office of the Chief Information Officer conducted an extensive review of NCUA's information security program this year. This along with the FISMA audit resulted in the OIG reporting the following seven information security program areas in which NCUA needs to make improvements: configuration management, incident response, and contingency planning programs; account management, plan of action and milestones, and oversight of contractor systems; and documenting program controls in its system security plan. We made 23 recommendations which would help NCUA continue to improve the effectiveness of its information security program. We have included NCUA's comments in their entirety at Appendix A.

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

II. BACKGROUND

This section provides background information on the Federal Information Security Modernization Act of 2014 (FISMA 2014) and the National Credit Union Administration (NCUA).

Federal Information Security Modernization Act of 2014

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 charged the Office of Management and Budget (OMB) with oversight of information security policies and practices.

On December 18, 2014, the President signed into law the Federal Information Security Modernization Act of 2014 (FISMA 2014) (Public Law 113-283), which reformed FISMA. FISMA 2014 authorizes the Secretary of the Department of Homeland Security (DHS) to assist the OMB Director in administering the implementation of agency information and security practices for federal information systems. Among other changes, FISMA 2014 also:

- Changes agency reporting requirements, modifying the scope of reportable information from primarily policies and financial information to specific information about threats, security incidents, and compliance with security requirements.
- Updates FISMA to address cyber breach notification requirements.
- Required the OMB Director to – within one year of the enactment of FISMA 2014 – revise Budget Circular A-130 to eliminate inefficient or wasteful reporting.[1]

The Department of Homeland Security (DHS) issued the Fiscal Year (FY) 2016 reporting metrics, 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. On November 4, 2016, OMB issued Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirement (M-17-05). This memorandum provides agencies with FY 2016-2017

[1] OMB published the revised Circular A-130, Managing Information as a Strategic Resource, on July 28, 2016.

Federal Information Security Modernization Act and Privacy Management reporting guidance and deadlines as required by FISMA 2104.

National Credit Union Administration (NCUA)

NCUA is the independent federal agency that charters, supervises, and insures the nation's federal credit unions. NCUA also insures many state-chartered credit unions. 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 (NCUA Board) consisting of a chairman and two members. The President of the United States appoints the members of the board and the Senate confirms the board members. 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 meets regularly each month in Alexandria, Virginia in open session, with the exception of August.

III. OBJECTIVE

The audit objective was to perform an independent evaluation of NCUA information security and privacy management policies and procedures for compliance with FISMA 2014 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 2014; and
- Remediating prior audit weaknesses pertaining to FISMA 2014 and other information security and privacy weaknesses identified.

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 reporting by the OIG.

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 2014, the E-Government Act, National Institute of Standards and Technology's (NIST) standards and guidelines, the Privacy Act, and OMB memoranda and information security and privacy policies.

During this audit, we assessed NCUA's information security program domains as identified in The Department of Homeland Security's FY 2016 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics (V1.1.3). This year's reporting metrics are organized around the five information security functions outlined in the NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework). These functions and corresponding metric domains included:

- Identify:
  - Risk Management and
  - Contractor Systems

- Protect:
  - Configuration Management,
  - Identity and Access Management, and
  - Security and Privacy Training

- Detect: Information Security
  - Continuous Monitoring

- Respond:
  - Incident Response

- Recover:
  - Contingency Planning

We also assessed NCUA's privacy management program.

We conducted our fieldwork from August 2016 through October 2016. 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 addressed or is in the process of addressing its prior year deficiencies as indicated in response to the 2015 FISMA report. NCUA has one remaining partial finding pertaining to an unsupported software component, which the agency will not be able to resolve in the timeline as previously indicated. We identified seven new information security areas for improvement as follows: account management, configuration management, incident response, oversight of contractor systems, plan of action and milestones, system security plan, and contingency planning. We discuss the unresolved prior year findings and these new issues below.

1. NCUA Needs to Improve Account Management Controls

We noted account management issues specific to controls over State Supervisory Authority (SSA) Examiner Accounts accessing NCUA resources, and with controls over NCUA network accounts and NCUA application accounts. We discuss these issues separately below.

State Supervisory Authority (SSA) Examiner Accounts

NCUA allows State Supervisory Authority examiners access to NCUA information systems resources [redacted]. Specifically:

- NCUA does not [redacted]. This issue is exacerbated because NCUA provides [redacted].

- The [redacted]. For example, [redacted].

In addition, NCUA procedures for provisioning SSA examiners with access to NCUA's network resulted in [redacted]

National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* (April 2013) requires organizations to implement multifactor authentication for local and network access to privileged and non-privileged accounts. NIST indicates that organizations can satisfy this requirement by complying with the requirements in Homeland Security Presidential Directive 12 (HSPD-12).

Homeland Security Presidential Directive 12: *Policy for a Common Identification Standard for Federal Employees and Contractors* (August 27, 2004) requires the use of PIV for gaining logical access to federally controlled information systems.

In addition, NIST SP 800-53, Revision 4, *AC-6 – Least Privilege*, states organizations are to employ the principle of least privilege, allowing only authorized accesses for users (or processes acting on behalf of users) which are necessary to accomplish assigned tasks in accordance with organizational missions and business functions.

- *AC-6, Control Enhancement (5) Least Privilege/Privileged Accounts* states the organization is to restrict privileged accounts on the information system to organization-defined personnel or roles.

- The Supplemental Guidance states restricting privileged accounts to specific personnel or roles prevents day-to-day users from having access to privileged information/functions.

NCUA Identity and Access Management Procedures, Version 1.1, July 8, 2015:

- Section 5.4 states the concept of least privilege requires that users should be able to access only the system resources needed to fulfill their job responsibilities.

- Section 5.9.7 states NCUA policy requires users (including application accounts) to change their passwords [redacted].

- Section 5.1.6 states Office of Chief Information Officer (OCIO) Information Technology (IT) Help Desk team is to review accounts [redacted] ensure that the passwords are changed, or that there is a valid approval [redacted].

NCUA provides the SSA examiners a choice of using: [redacted] NCUA management indicated it provided these options because some of the SSAs have [redacted]; and to ensure all SSA examiners had the equipment to perform examinations and exchange examination information with NCUA.

Management indicated that the SSA examiners [redacted] However, OCIO management indicated there are alternative means for allowing users [redacted] if necessary.

Management indicated NCUA has not [redacted]

NCUA provides SSA examiners with access to the NCUA network to upload or download sensitive credit union information as part of the NCUA examination process. [redacted], NCUA could mitigate the risk(s) that SSA examiners could inadvertently introduce vulnerabilities into the NCUA infrastructure.

Regarding SSA examiner accounts [redacted]

By requiring SSA examiners to [redacted] NCUA can mitigate the risk(s) of unauthorized access and the introduction of vulnerabilities to the NCUA network. Ultimately, NCUA can help ensure the confidentiality, integrity, and availability of sensitive information on laptops and the NCUA network.

We recommend that:

1. NCUA assess the current process and alternative strategies [redacted] that mitigates the current risk(s) to the NCUA infrastructure.

Agency Response:

NCUA concurred with our recommendation. Management indicated the Office of Examination and Insurance (E&I), Office of Continuity and Security Management (OCSM), and the Office of the Chief Information Officer (OCIO) will jointly assess the current process and alternative strategies for [redacted]

[redacted] mitigates the current risk(s) to the NCUA infrastructure by December 31, 2018.

OIG Response:

We concur with management's planned actions.

2. OCIO implement a process [redacted] in accordance with agency policy.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement a process [redacted] in accordance with agency policy by June 30, 2017.

OIG Response:

We concur with management's planned action.

NCUA Network Accounts

We noted NCUA network account management issues pertaining to inactive accounts, [redacted] account approval, new hire account authorizations, and approvals for remote access. Specifically, we identified the following issues:

Inactive Accounts: NCUA [redacted] accounts are [redacted]. We identified two [redacted].

NIST SP 800-53, Revision 4, *IA-4 – Identifier Management*, states organizations are to manage information system identifiers by disabling the identifier after an organization-defined time period of inactivity.

NCUA Identity and Access Management Procedures, Version 1.1, July 8, 2015, Section 5.1.7 states [redacted].

NCUA's process for reviewing [redacted] OCIO management indicated it plans [redacted].

[redacted] Approval: None of the three [redacted] accounts we sampled had evidence of account approval.

NIST SP 800-53, Revision 4, *AC-2 – Account Management*, states organizations are to require approvals by personnel to create information system accounts.[2]

NCUA Identity and Access Management Procedures, Version 1.1, July 8, 2015, Section 5.1.4.2 states Office of Chief Information Officer (OCIO) Domain Admins [redacted] accounts on an as needed basis based on management approval.

NCUA management indicated that although the approvals [redacted] accounts were communicated, OCIO did not document the approvals.

New Hire Account Authorization: One of the eight new hires we sampled for testing did not complete the Rules of Behavior (ROB) within the 10-day window required by NCUA, retaining access to the network for 11 months without reviewing the ROB.

NIST SP 800-53, Revision 4, *PS-6 – Access Agreement*, states organizations are to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

NCUA Identity and Access Management Procedures, Version 1.1, July 8, 2015, Section 5.1.4.1 states users complete NCUA Rules of Behavior (equivalent to general security awareness training) within 10 business days of Entry On [sic] Duty date.

Management indicated it was an oversight that a new hire retained network access for 11 months without reviewing the rules of behavior. In addition, the *NCUA Identity and Access Management Procedures* policy does not address the ramifications of not completing the ROB within the 10-day window, such as disabling network access.

Remote Access Approval: One of the 11 remote [redacted] accounts we sampled for testing did not have evidence of account approval. This account [redacted].

NIST SP 800-53, Revision 4, *AC-17 – Remote Access*, states organizations are to establish and document usage restrictions, configuration/connection requirements, and implementation guidance for each type of remote access allowed and authorize remote access to the information system prior to allowing such connections.

NCUA Remote Access Procedure Version 1.1, January 2015, specifies remote access is [redacted] to allow users to work remotely as needed, and to

[2] Information system account types include, for example, individual, shared, group, system, guest/anonymous, emergency, developer/manufacturer/vendor, temporary, and service.

support telework arrangements. Remote access is granted [redacted]. Requests must come from [redacted]

OCIO Management indicated that the process for OCIO's approval [redacted] remote access was verbal and not based on a written request as required.

Implementing and enforcing effective account management controls mitigates the risk(s) of granting inappropriate access and privileges, which could ultimately lead to unauthorized modification, loss, or disclosure of sensitive NCUA information.

We recommend that OCIO:

3. Implement a process [redacted] in accordance with agency policy.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement a process [redacted] in accordance with agency policy by March 31, 2017.

OIG Response:

We concur with management's planned action.

4. Enforce its *Identity and Access Management Procedures* policy for ensuring access approvals are completed and maintained for [redacted] accounts.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will enforce the *Identity and Access Management Procedures* policy for ensuring access approvals are completed and maintained for [redacted] accounts by March 31, 2017.

OIG Response:

We concur with management's planned action.

5. Update the *NCUA Identity and Access Management Procedures* policy to address the consequence of new hires not completing the Rules of Behavior within the required 10-day window of entry on duty and enforce the specified consequence.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will update the *NCUA Identity and Access Management Procedures* to address the consequence of new hires not completing the Rules of Behavior within the required 10 day window of entry on duty and enforce the specified consequence by December 31, 2017.

OIG Response:

We concur with management's planned actions.

6. Enforce the *NCUA Identity and Access Management Procedures* policy to ensure remote access [redacted] is approved.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will enforce the *NCUA Identity and Access Management Procedures* to ensure remote access [redacted] is approved by December 31, 2016.

OIG Response:

We concur with management's planned action.

NCUA Applications' Accounts

We noted user Account Management controls were not in place [redacted] after a period of inactivity.

NIST SP 800-53, Revision 4, *AC-2 – Account Management*, states organizations are to disable and remove information system accounts in accordance with organization-defined procedures. NIST SP 800-53 AC-2 also states the information system *automatically* [emphasis added] disables inactive accounts after an organization-defined time period.

NCUA Identity and Access Management Procedures, Version 1.1, July 8, 2015, Section 5.1.7 states [redacted].

The *NCUA Identity and Access Management Procedures* document does not address a policy for [redacted]

[redacted]

By appropriately and timely [redacted], NCUA can mitigate the risk of unauthorized access to this system and the risk(s) to the confidentiality, integrity, and availability of sensitive NCUA information.

We recommend that:

7. OCIO work with E&I management to determine appropriate policies for [redacted] and update the *NCUA Identity and Access Management Procedures* accordingly.

   Agency Response:

   NCUA concurred with our recommendation. Management indicated E&I and OCIO will determine appropriate policies for [redacted] and update the *NCUA Identity and Access Management Procedures* accordingly by March 31, 2017.

   OIG Response:

   We concur with management's planned actions.

8. E&I management document and work with OCIO to implement [redacted] in accordance with NCUA policy.

   Agency Response:

   NCUA concurred with our recommendation. Management indicated OCIO will implement [redacted] in accordance with NCUA policy by September 30, 2017.

   OIG Response:

   We concur with management's planned action.

2. NCUA Needs to Improve its Controls over its Configuration Management Program

We noted issues with NCUA's configuration management program in the areas of Baseline Configuration, Software Inventory, Patch Management, and Unsupported Software, We discuss each of these issues below.

Baseline Configuration:
NCUA did not fully implement [redacted] identified by management as the standard baseline configuration policy for [redacted]

NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4:

- *CM-2, Baseline Configuration*, states organizations are to develop, document, and maintain under configuration control, a current baseline configuration of the information system.
- *CM-6, Configuration Settings*, states organizations are to implement the configuration settings, identify, document, and approve any deviations from established configuration settings for information system components based on organization-defined operational requirements.

NCUA Configuration Management Plan and Procedures, Version 1.1, April 2, 2015, 7.4 Updating Configuration Settings and Configuration Baselines, states all NCUA information systems under development and in production must document and maintain under configuration control a current baseline configuration of the information system.

OCIO management indicated that this year, NCUA adopted [redacted] after determining NCUA lacked a standard baseline configuration model [redacted] configuration standards established by the Federal Desktop Core Configuration[4] (FDCC) and the United States Government Configuration Baseline[5] (USCGB). In addition, OCIO management indicated that its implementation strategy is to first implement the configuration standards in its non-production environment to ensure resilience of the standards within NCUA's operating environment, followed by implementing the standards in the production environment. Furthermore, [redacted]

[3] [redacted]

[4] Federal Desktop Core Configuration (FDCC) is a checklist for mandatory configuration settings on desktop and laptop computers owned by the United States government.

[5] The purpose of the United States Government Configuration Baseline (USGCB) initiative is to create security configuration baselines for Information Technology products widely deployed across the federal agencies. The USGCB baseline evolved from the Federal Desktop Core Configuration mandate.

By implementing proper security configuration baselines, NCUA will have reasonable assurance its systems are more secure and no unknown deviations from the baseline have been introduced. Ultimately, this will help NCUA mitigage the risk(s) to the confidentiality, integrity, and availability of sensitive NCUA information.

Software Inventory:
NCUA does not have a complete inventory of its approved software. Although the inventory included the standard software installed on every workstation (i.e., the Gold image), it did not include additional software that NCUA has approved outside of the Gold image. In addition, [redacted]

NIST SP 800-53, Revision 4, *CM-8 – Information System Component Inventory*, states organizations are to develop and document an inventory of information system components that accurately reflects the current information system. The inventory should include all components within the authorization boundary of the information system, is at the level of granularity deemed necessary for tracking and reporting; and is reviewed and updated on an organization-defined frequency.

- CM-8(3)(a) states organizations are to employ automated mechanisms to detect the presence of unauthorized hardware, software, and firmware components within the information system.

- CM-8(3)(b), states when unauthorized components are detected, organizations are to disable network access by such components, isolate the components, and notify organization-defined personnel or roles.

NCUA Configuration Management Plan and Procedures, Version 1.1, April 2, 2015, Section 6 states NCUA's parts and equipment inventory [redacted] and is updated as equipment is added to, or removed from, use. NCUA individually accounts for every NCUA computing resource (e.g., desktops, laptops, servers, portable electronic devices, commercial off-the-shelf [COTS] software packages, and applications) as part of a recognized information system inventory.

OCIO management indicated users can [redacted] However, NCUA does not capture this software on its list of approved software. In addition, since users are not able to download software on their laptops on their own, e.g., unauthorized software, [redacted].

[redacted] NCUA will have reasonable assurance its systems are less susceptible to known or future vulnerabilities and exploits.

Patch Management:
NCUA did not track, test or approve [redacted] patches installed on [redacted] [redacted].

NIST SP 800-53, Revision 4, *SI-2, Flaw Remediation*, states organizations are to test software and firmware updates related to flaw remediation for effectiveness and potential side effects before installation.

NIST SP 800-40, Revision 3, *Guide to Enterprise Patch Management Technologies*, July 2013, states installing a patch may "break" other applications; this can best be addressed by testing patches before deployment.

NCUA Configuration Management Plan and Procedures, Version 1.1, April 2, 2015, Section 20 states OCIO [redacted]

OCIO management indicated OCIO staff members were not following NCUA policy that requires testing [redacted] patches [redacted] [redacted]. OCIO staff members were only tracking, testing and approving [redacted].

By appropriately testing patches [redacted], NCUA will have reasonable assurance of patch integrity and reduce the potential risk of introducing errors to the NCUA environment.

Unsupported Software:
NCUA has three instances [redacted] [redacted]. We documented NCUA's unsupported software during our FISMA 2015 audit, and these are the remaining instances of unsupported software. As we reported last year, mainstream support for this software [redacted], and extended support that NCUA purchased [redacted].

Revision of Office of Management and Budget, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1 states agencies are to prohibit the use of unsupported information systems and system components, and ensure that systems and components that cannot be appropriately protected or secured are given a high priority for upgrade or replacement.

NIST Special Publication 800-53, Revision 4, *SA-22, Unsupported Software Components*, requires organizations to replace information system components when support for the components is no longer available from the developer, vendor, or manufacturer. Support for information system components includes, for example, software patches, firmware updates, replacement parts, and maintenance contracts. Exceptions to replacing unsupported system components may include, for example, systems that provide critical mission/business capability where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

OCIO Management indicated its timeline for replacing [redacted]

By replacing unsupported software and components within its infrastructure in a timely manner, NCUA will have reasonable assurance that: (1) its systems are not susceptible to old or new vulnerabilities and exploits that the vendors have addressed with current supported versions; and (2) it will receive continued support from the vendors against future vulnerabilities and exploits. Ultimately, NCUA will – on a continuous basis – more effectively protect its infrastructure and sensitive NCUA and credit union information against potential compromise.

Recommendations:

We recommend that OCIO:

9. Configure its [redacted] standard baseline.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will configure [redacted] standard baseline [redacted].

OIG Response:

We concur with management's planned actions.

10. Implement a process to ensure NCUA maintains a complete inventory of all approved software.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement a process to ensure NCUA maintains a complete inventory of all approved software by June 30, 2017.

OIG Response:

We concur with management's planned action.

11. Implement [redacted].

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement [redacted]

OIG Response:

We concur with management's planned action.

12. Implement a process to ensure NCUA tracks, tests, and approves [redacted] patches [redacted].

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement a process to ensure NCUA tracks, tests, and approves [redacted] patches [redacted]

OIG Response:

We concur with management's planned action.

13. Complete the decommissioning [redacted] according to the schedule management specified.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will complete the decommissioning [redacted].

OIG Response:

We concur with management's planned action and note that management extended its scheduled decommissioning date [redacted] as indicated in the report.

3. NCUA needs to Improve its Incident Response Program

NCUA did not properly maintain the ongoing status of its security incident remediation activities. Specifically, of the 12 security incidents we sampled for testing, NCUA did not provide documented evidence that it tracked and updated the status of each activity taken to remediate the incidents.

NIST Special Publication (SP) 800-53, *Security and Privacy Controls for Federal Information Systems and Organizations*, Revision 4, IR-5 Incident Monitoring, states organizations are to track and document information system security incidents. In addition, the *Supplemental Guidance* states documenting information system security incidents includes, for example, maintaining records about each incident, the status of the incident, and other pertinent information necessary for forensics.

NCUA Security Incident Response Procedure, Version 1.2, July 15, 2015, Section 5.3 states the severity of an incident and its impact or threat to the operation or integrity of the NCUA determines the route of the notification process. Personnel will adhere to the following guidelines when notifying key personnel of the occurrence of incidents, any updates necessary, and the remediation of the incident(s).

- [redacted]
- [redacted]
- [redacted]
- [redacted]
- [redacted]

Management indicated the incident tracking tool it was using did not properly record the audit trail of updates to remediation activities through resolution of the incident. The tool only recorded the last action taken. At the completion of our testing, management informed us they procured and are in the process of implementing an IT Service Management solution, which allows the agency to fully manage events, incidents, problems, and breaches. The solution will automate notifications to key personnel regarding the status of remediation activities in accordance with the policy. [redacted]

By properly recording status updates to remediation activities, management can have increased confidence that the agency is properly handling and closing security incidents in a timely manner, lessening the impact of vulnerabilities on the NCUA information system environment. In addition, by tracking detailed incident response activities, management will be able to assess lessons learned regarding the remediation process and how quickly it is able to respond to, remediate, and resolve various incidents. This can be useful information for incident response training, process improvements, and trend analysis.

Recommendation:

We recommend that OCIO:

14. Implement [redacted] IT Service Management solution for managing security incidents.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement [redacted] IT Service Management solution for managing security incidents [redacted].

OIG Response:

We concur with management's planned action.

4. NCUA Needs to Improve its Risk Management Program

NCUA has made significant progress to address last year's FISMA finding that the agency had not defined and communicated an organization-wide risk tolerance. However, although NCUA's organization-wide risk tolerance is mostly completed, it does not include the degrees of risk uncertainty that are acceptable. Without the completed organization-wide risk tolerance, OCIO does not have the organizational risk framework it needs to re-align its current information system risk tolerance as we also reported last year.

NIST SP 800-39, Revision 1, *Managing Information Security Risk Organization, Mission, and Information System View* (March 2011) states: The first component of risk management addresses how organizations frame risk or establish a risk context—that is, describing the environment in which risk-based decisions are made. The risk frame establishes a foundation for managing risk and delineates the boundaries for risk-based decisions within organizations. Establishing a realistic and credible risk frame requires that organizations identify: (i) risk assumptions (e.g., assumptions about the threats, vulnerabilities, consequences/impact, and likelihood of occurrence that affect how risk is assessed, responded to, and monitored over time); (ii) risk constraints (e.g., constraints on the risk assessment, response, and monitoring alternatives under consideration); (iii) risk tolerance (e.g., levels of risk, types of risk, and degree of risk uncertainty that are acceptable); and (iv) priorities and trade-offs (e.g., the relative importance of missions/business functions, trade-offs among different types of risk that organizations face, time frames in which organizations must address risk, and any factors of uncertainty that organizations consider in risk responses).

NIST SP 800-53 Revision 4, *PM-9, Risk Management Strategy*, states that organizations are to develop a comprehensive strategy to manage risk to organizational operations and assets, individuals, other organizations and the Nation associated with the operation and use of information systems; implement the risk management strategy consistently across the organization; and review and update the risk management strategy at a defined frequency or as required to address organizational changes. An organization-wide risk management strategy clearly communicates the risk tolerance for the organization, acceptable risk assessment methodologies, risk mitigation strategies, a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance, and approaches for monitoring risk over time.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems* (February 2010) indicates that: An organization's risk executive (function) helps to ensure: (i) risk-related considerations for individual information systems, to include authorization decisions, are viewed from an organization-wide perspective with regard to the overall strategic goals and objectives of the organization in carrying out its core missions and business functions; and (ii) managing information system-related security risks is consistent across the organization, reflects organizational risk tolerance, and is considered along with other types of risks in order to ensure mission/business success.

In FY 2015, NCUA implemented an agency level Enterprise Risk Management Council. This year the Enterprise Risk Management Council developed and documented the majority of the elements of an organization-wide risk tolerance (i.e., the levels of risk and types of risk, a risk appetite statement, the risk appetite scale, the impact rating scale, and the risk management taxonomy). When we reviewed NCUA's organization-wide risk tolerance, we apprised the agency that in order to complete the risk tolerance, it needs to also include the degree of risk of uncertainty.

Once NCUA completes and communicates a comprehensive organization-wide risk tolerance, OCIO will be able to align its strategic goals, objectives, and requirements for protecting its information and information systems with the risk tolerance that supports NCUA's mission and business success. Ultimately, this would help to ensure OCIO consistently manages and monitors information security-related risks related to the confidentiality, integrity, and availability of sensitive agency and credit union information.

Recommendations:

We recommend that:

15. NCUA finalize its organizational-wide risk tolerance by incorporating the degree of risk of uncertainty and communicate the risk tolerance organization-wide.

Agency Response:

NCUA concurred with our recommendation. Management indicated the Office of the Chief Financial Officer (OCFO) will finalize NCUA's organizational-wide risk tolerance by incorporating the degree of risk of uncertainty and communicate the risk tolerance organization-wide by September 30, 2017.

OIG Response:

We concur with management's planned actions.

16. OCIO re-align its current information system risk tolerance with the organization-wide risk tolerance.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will align its current information system risk tolerance with the organization-wide risk tolerance by September 30, 2017.

OIG Response:

We concur with management's planned action.

5. NCUA needs to Improve its Oversight of Contractor Systems[6]

NCUA did not conduct a risk assessment for seven of 25 contractor systems. Specifically, NCUA did not conduct initial risk assessments prior to using the following seven

[6] Contractor systems include systems operated on behalf of an organization by contractors or other entities, including other government agencies, managed hosting environments, and systems and services residing in a cloud external to the organization.

contractor-owned and operated or government-owned and operated systems:

[redacted]

NIST 800-37, Revision 1, states the risk management framework emphasizes maintaining awareness of the security state of information systems on an ongoing basis though enhanced monitoring processes; and providing essential information to senior leaders to facilitate decisions regarding the acceptance of risk to the organization arising from the operation and use of information systems. FISMA and OMB policy require external providers handling federal information or operating information systems on behalf of the federal government to meet the same security requirements as federal agencies.

NIST 800-37 (Revision 1) also indicates organizations can choose from three different approaches when planning for and conducting security authorizations to include: (i) an authorization with a single authorizing official; (ii) an authorization with multiple authorizing officials; or (iii) leveraging an existing authorization. In leveraging existing authorizations, an organization chooses to accept some or all of the information in an existing authorization package generated by another federal agency (hereafter referred to as the owning organization) based on a need to use the owning organization's authorization package as the basis for determining risk to the leveraging organization. When reviewing the authorization package, the leveraging organization considers risk factors such as the time elapsed since the authorization results were produced, the environment of operation (if different from the environment of operation reflected in the authorization package), the criticality/sensitivity of the information to be processed, stored, or transmitted, as well as the overall risk tolerance of the leveraging organization. If the leveraging organization determines that there is insufficient information in the authorization package or inadequate security measures in place for establishing an acceptable level of risk, the leveraging organization may negotiate with the owning organization for additional security measures and/or security-related information.

[7] [redacted]

NCUA Contractor Systems Oversight Procedures, Version 2.0, April 9, 2015, indicates:

- Before contracts are awarded, the OCIO IT Security team performs an information security risk review for each eligible contractor to determine information security risks associated with the contractor, contractor systems and services, and will be the basis of OCIO's authorization of the system to operate if contract is awarded.

- If available, OCIO will review the full ATO[8] package of another federal agency to assess the risk associated with operating the system in support of NCUA and identifying compensating controls OCIO needs [sic] implement to mitigate unacceptable weaknesses and vulnerabilities. This review will be the basis of determining if accepting the risk to operate the system is appropriate.

OCIO management indicated it did not initially assess the specific risk(s) to NCUA for the government owned and operated systems because NCUA placed full reliance on the ATOs (authorities to operate) granted by the federal agencies that own and operate them. In addition, NCUA management indicated it did not have a coordinated process for obtaining input from the Program Offices on these systems. Furthermore, OCIO management indicated that it did not start the initial risk assessments for these systems this year because OCIO lacked the time and resources necessary to complete the assessments.

By adequately assessing, documenting, and formally accepting risk for contractor systems, NCUA can have reasonable assurance that it appropriately identifies and considers potential threats and control weaknesses posed by these systems. In addition, NCUA can implement appropriate compensating controls as necessary to help mitigate residual risks resulting from the use of contractor systems. Ultimately, NCUA can mitigate the overall risks of unauthorized access, and modification or disclosure of sensitive agency information created by NCUA's use of contractor systems.

Recommendations:

We recommend that OCIO:

17. Coordinate developing, documenting, and implementing a process to ensure Program Offices notify OCIO of contractor systems early within the procurement process to allow completion of a risk assessment before the system is permitted to operate within NCUA's information system environment.

[8] Authority to Operate.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will implement a process to ensure Program Offices notify OCIO of contractor systems early within the procurement process to allow completion of a risk assessment before the system is permitted to operate within NCUA's information system environment by December 31, 2017.

OIG Response:

We concur with management's planned action.

18. Enforce policy to ensure it assesses risk(s) for all contractor systems and documents and formally accepts residual risk(s) to the agency prior to initial use.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will enforce policy to ensure it assesses risk(s) for all contractor systems and documents and formally accepts residual risks to the agency prior to initial use by March 31, 2018.

OIG Response:

We concur with management's planned actions.

6. NCUA needs to Improve its Plan of Action and Milestones Management Process

NCUA did not complete the documentation of the majority of its Plan of Action and Milestones (POA&M) items. Specifically, we noted the following deficiencies in NCUA's general, system specific, and Credit Union Service Organization (CUSO) POA&Ms:

- NCUA did not document a corrective action plan for 297 of 304 NCUA general POA&Ms;
- NCUA did not document a scheduled completion date for 114 of 304 general POA&M items;
- NCUA did not document a justification for missed estimated completion dates in the milestone updates for 14 general POA&M items;
- NCUA did not document a justification for missed estimated completion dates in the milestone updates for the entire population of system specific POA&M items;

- NCUA did not document a scheduled completion date, the responsible party, or the milestone updates for the entire population of the Credit Union Service Organization (CUSO) Registry System POA&M items;

- NCUA did not document estimated funding resources required to resolve the weaknesses for the entire population of POA&M items;

- NCUA indicated that POA&M items past their scheduled completion dates were on-track or at risk instead of annotating them as past due; and

- From a sample of five closed POA&M items, NCUA did not document evidence that the weakness for three of those closed POA&Ms was remediated and validated for closure.

NIST SP 800-53, Revision 4, *CA-5 – Plan of Action and Milestones*, states organizations are to develop a plan of action and milestones 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 plan of action and milestones on an organization-defined frequency based on the findings from security controls assessments, security impact analyses, and continuous monitoring activities.

NIST SP 800-37, Revision 1 states to facilitate the near real-time management of risk associated with the operation and use of the information system, the organization updates the security plan, security assessment report, and plan of action and milestones on an ongoing basis. The information provided by these key updates helps to raise awareness of the current security state of the information system thereby supporting the process of ongoing authorization and near real-time risk management. The updated plan of action and milestones reports progress made on the current outstanding items listed in the plan.

NCUA's *Office of the Chief Information Officer (OCIO) Plan of Action and Milestones (POA&M) Policy and Procedures* (August 11, 2015), requires weaknesses and remediation action plans to be documented in the POA&M tracker. The policy states that the information in the POA&M should be maintained continuously and a regular update should be provided to the Chief Information (CIO) and Deputy Chief Information Officer (DCIO) to communicate overall progress in identifying and mitigating weaknesses. Changes to POA&M due dates will be discussed at the OCIO risk review board meeting and/or the director's meeting. The policy also states weaknesses should be considered "Completed" only when they have been fully resolved and the corrective action has been tested. Testing completed weaknesses demonstrates that the program vulnerability or system control has been adequately addressed and proven effective. This step should be explicitly incorporated into the weakness mitigation process and documented accordingly.

During FY 2015, NCUA hired a new Chief Information Security Officer (CISO) to oversee the NCUA information security program. The new CISO led a comprehensive internal assessment of the NCUA information security program and listed the identified weaknesses or deficiencies in the POA&M tracking system. OCIO focused its efforts – during the new CISO's early tenure – on *identifying* and *recording* the agency's security program issues and concerns as illustrated by the high number of POA&M items, without sufficient time or adequate resources to concurrently work on *completing* the POA&M data. In addition, NCUA's POA&M policy does not address timelines for completing the documentation of POA&M items or for updating its POA&M items to facilitate near real-time management of risk(s) associated with the operation and use of agency information systems.

For the three sampled closed POA&Ms, management indicated staff members validated the POA&M items by observing the resolutions, but did not follow NCUA policy, which requires documenting the evidence of the remediation.

By fully documenting the organization's planned remedial actions for each POA&M item and also maintaining the current status of the POA&M items, NCUA can more effectively manage system security risks to the confidentiality, integrity, and availability of the agency's systems and data on a near real-time basis. In addition, documenting remediation steps – regardless of the method(s) of remediation – helps NCUA management and staff to validate that the remediation is appropriate, properly tested and effective, decreasing the risk that weaknesses still exist.

Recommendations:

We recommend that OCIO:

19. Update the *Office of the Chief Information Officer (OCIO) Plan of Action and Milestones (POA&M) Policy and Procedures* to address reasonable timelines within which the agency must fully document and update its POA&M items on an ongoing basis.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will update the POA&M Policy and Procedures to address reasonable timelines within which the agency must be fully document and update its POA&M items on an ongoing basis by December 31, 2017.

OIG Response:

We concur with management's planned action.

20. Enforce NCUA policy to ensure the agency appropriately and timely documents and updates POA&M items to reflect the current status on an ongoing basis, and the agency tests, validates, and documents corrective actions in order to close POA&Ms.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will enforce its policy to ensure the agency appropriately and timely documents and updates POA&M items to reflect the current status on an ongoing basis, and the agency tests, validates and documents corrective actions in order to close POA&Ms by March 31, 2018.

OIG Response:

We concur with management's planned actions.

7. NCUA needs to Improve its General Support System (GSS) Systems Security Plan

NCUA's General Support System (GSS) Systems Security Plan (SSP) does not fully document required NIST controls. Specifically the SSP does not address the privacy [redacted] controls as described by NIST. The issue regarding privacy controls is part of the prior year Privacy Program finding, which we address later in the report. We include a brief explanation of this issue below.

NIST SP 800-53, Revision 4, states the system security plan provides an overview of the security requirements of the information system and describes the controls in place or planned for meeting those requirements. In addition to security controls, NIST 800-53 describes privacy controls [redacted]. [redacted]

According to Revision of OMB, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, all selected security controls must be documented in an information system security plan and implemented.

OCIO management indicated it deferred updating the NCUA's GSS SSP pending: [redacted] the Senior Agency Official for Privacy's (SAOP) establishment of the agency's privacy program. OCIO management added that it expected the vast majority [redacted]. OCIO management further stated it is in the process of updating agency security documentation in conjunction with the new GSS authorization to operate, which management indicated is currently in progress.

As stated above, we address the prior year issue regarding the privacy program and associated privacy controls under the Privacy Program finding later in the report. NCUA management indicates it is on track to complete its privacy program and associated controls by December 31, 2016, which is the timeline NCUA management provided in response to the 2015 FISMA report. NCUA management also responded in that report that it would incorporate the privacy controls into the agency's system security plan by March 31, 2017. Therefore, we are not making an additional recommendation regarding the privacy controls at this time.

NIST SP 800-53 periodically publishes revisions to their control baselines and standards to address new risks in today's information system environment. By updating its system security plan to also address the privacy [redacted] controls as described by NIST to reflect current control standards applicable to NCUA, the agency can reduce the susceptibility of its information and information systems to new and heightened security risks, such as unauthorized access, viruses, malicious code, and exploitable vulnerabilities.

Recommendation:

We recommend that:

21. OCIO update the system security plan for the general support system [redacted] in accordance with NIST SP 800-53.

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will update the system security plan for the general support system [redacted] in accordance with NIST SP 800-53 by December 31, 2017.

OIG Response:

We concur with management's planned action.

8. NCUA needs to Improve its Contingency Planning Program

NCUA has not conducted an agency Business Impact Analysis (BIA) [redacted]. As a result, [redacted]

NIST SP 800-53, Revision 4, *CP-2, Contingency Planning*, states organizations are to identify essential missions and business functions, and associated contingency requirements. Control enhancement (3) states organizations are to plan for the resumption of essential missions and business functions within an organization-defined time period of contingency plan activation; and control enhancement (8) states organizations are to identify critical information system assets supporting essential missions and business functions.

NIST Special Publication (SP) 800-34, *Contingency Planning Guide for Federal Information Systems*, Revision 1 (May 2010) states the BIA is a key step in implementing the CP controls in NIST SP 800-53 and in the contingency planning process overall. 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. Three steps are typically involved in accomplishing the BIA:

- Determine mission/business processes and recovery criticality.
- Identify resource requirements.
- Identify recovery priorities for system resources.

NCUA Information Security Policy Handbook, Version 1.7, August 11, 2015, Section 6.5, states contingency plans identify critical assets (using the Business Impact Assessment (BIA)), key employees and vendors, and established procedures to respond to outages.

In January 2014, NCUA established the Office of Continuity and Security Management (OCSM) to strengthen and integrate the agency's continuity of operations (COOP), emergency management, and security programs. As part of the Federal Emergency Management Agency's audit of NCUA's COOP program in May 2014, OCSM established a working group that determined that the agency's Mission Essential Functions (MEFs) needed to be updated and validated prior to the agency conducting a formal Business Process Analysis (BPA)/BIA. The OCSM working group also determined that OCSM needed to identify and/or validate critical IT Systems requirements for all NCUA offices.

In August 2015, OCSM management indicated it submitted a request for funds to support contracted services to conduct a formal BPA/BIA; however, NCUA determined the newly enhanced OCSM staffing would lead the endeavor instead. In June 2016, OCSM initiated a process to address the need to: (a) validate NCUA's list of MEFs and (b) begin a BPA. OCSM management added that the proposal included sponsorship of a joint OCFO\OCSM Management Development Program (MDP) Project to work on completing the MEF review and to begin the BPA.

OCSM management indicated the MDP Team has developed the revised list of MEFs, which was coordinated with all regions/offices for comment, and subsequently approved by the

Executive Director in September 2016. OCSM management also indicated that it has begun the initial steps of the BPA and should complete them by the second quarter of 2017. NCUA management indicated OCSM may need to supplement their staffing resources in 2017 to follow up on the BPA results to conduct the BIA.

By formally identifying and documenting an agency BIA the critical agency mission/business processes and associated information systems, resource requirements, and [redacted]

Recommendations:

We recommend that:

22. OCSM complete the business process analysis, and conduct and document a formal business impact analysis to identify critical agency mission/business processes and associated information systems, resource requirements, [redacted].

Agency Response:

NCUA concurred with our recommendation. Management indicated OCSM will complete the business process analysis and conduct and document a formal business impact analysis to identify critical agency mission/business processes and associated information systems, resource requirements [redacted].

OIG Response:

We concur with management's planned actions.

23. OCIO update the NCUA GSS Contingency Plan to include the business impact analysis results [redacted]

Agency Response:

NCUA concurred with our recommendation. Management indicated OCIO will update the NCUA GSS Contingency Plan to include the business impact analysis results [redacted]

OIG Response:

We concur with management's planned action.

9. NCUA needs to Improve its Privacy Program

NCUA has made significant progress addressing last year's FISMA finding: The agency has documented – in draft format – the privacy policies and procedures and associated controls to support and monitor the organization-wide privacy program. However, NCUA has not finalized its privacy program and controls.

Last year the FISMA audit reported that:

- NCUA's existing privacy policies and procedures did not comprehensively address protecting and ensuring the proper handling of personally identifiable information (PII);
- NCUA had not fully documented controls associated with NCUA privacy policies and procedures for all programs, information systems, and technologies involving PII; and
- NCUA had not fully updated its General Support System Security Plan to address current NIST privacy controls.

Revision of Office of Management and Budget, Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1 states the Senior Agency Official for Privacy (SAOP) shall develop and maintain a privacy program plan that provides an overview of an agency's privacy program, including a description of the structure of the privacy program, the resources dedicated to the privacy program, the role of the SAOP and other privacy officials and staff, the strategic goals and objectives of the privacy program, and the program management controls and common controls in place or planned for meeting applicable privacy requirements and managing privacy risks.

NIST 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII)* (April 2010) states organizations are to develop comprehensive policies and procedures for handling PII at the organization level, the program or component level, and where appropriate, at the system level.

NIST SP 800-53, Revision 4, *AR-1 Governance and Privacy Program*, states organizations are to develop, disseminate, and implement operational privacy policies and procedures that govern the appropriate privacy and security controls for programs, information systems, or technologies involving PII. The Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO), in consultation with legal counsel, information security officials, and others as appropriate, ensures the development, implementation, and enforcement of privacy policies and procedures.

In addition NIST 800-53, Revision 4, Appendix J provides a structured set of controls for protecting privacy and serves as a roadmap for organizations to use in identifying and implementing privacy controls concerning the entire life cycle of PII, whether in paper or electronic form. The controls focus on information privacy as a value distinct from, but highly interrelated with, information security. Privacy controls are the administrative, technical, and physical safeguards employed within organizations to protect and ensure the proper handling of PII. Organizations may also engage in activities that do not involve the collection and use of PII, but may nevertheless raise privacy concerns and associated risk. The privacy controls are equally applicable to those activities and can be used to analyze the privacy risk and mitigate such risk when necessary. The privacy families can be implemented at the organization, department, agency, component, office, program, or information system level, under the leadership and oversight of the Senior Agency Official for Privacy (SAOP)/Chief Privacy Officer (CPO) and in coordination with the Chief Information Security Officer, Chief Information Officer, program officials, legal counsel, and others as appropriate.

OMB A-130, *Managing Information as a Strategic Resource*, states that a privacy plan is a formal document that details the privacy controls selected for an information system that are in place or planned. OMB A-130 also states that an information system's privacy plan and its system security plan may be integrated into one consolidated document.

NCUA has made significant progress establishing and developing its Privacy Program. NCUA management indicated the agency is on track to complete the documentation and implementation of the its privacy policies and procedures and associated controls by December 31, 2016, as indicated in response to the 2015 FISMA audit report. In addition, OCIO indicated in its response to the 2015 FISMA audit report that it would incorporate privacy controls in the system security plan by March 31, 2017. Therefore, we are not making any additional recommendations to NCUA at this time.

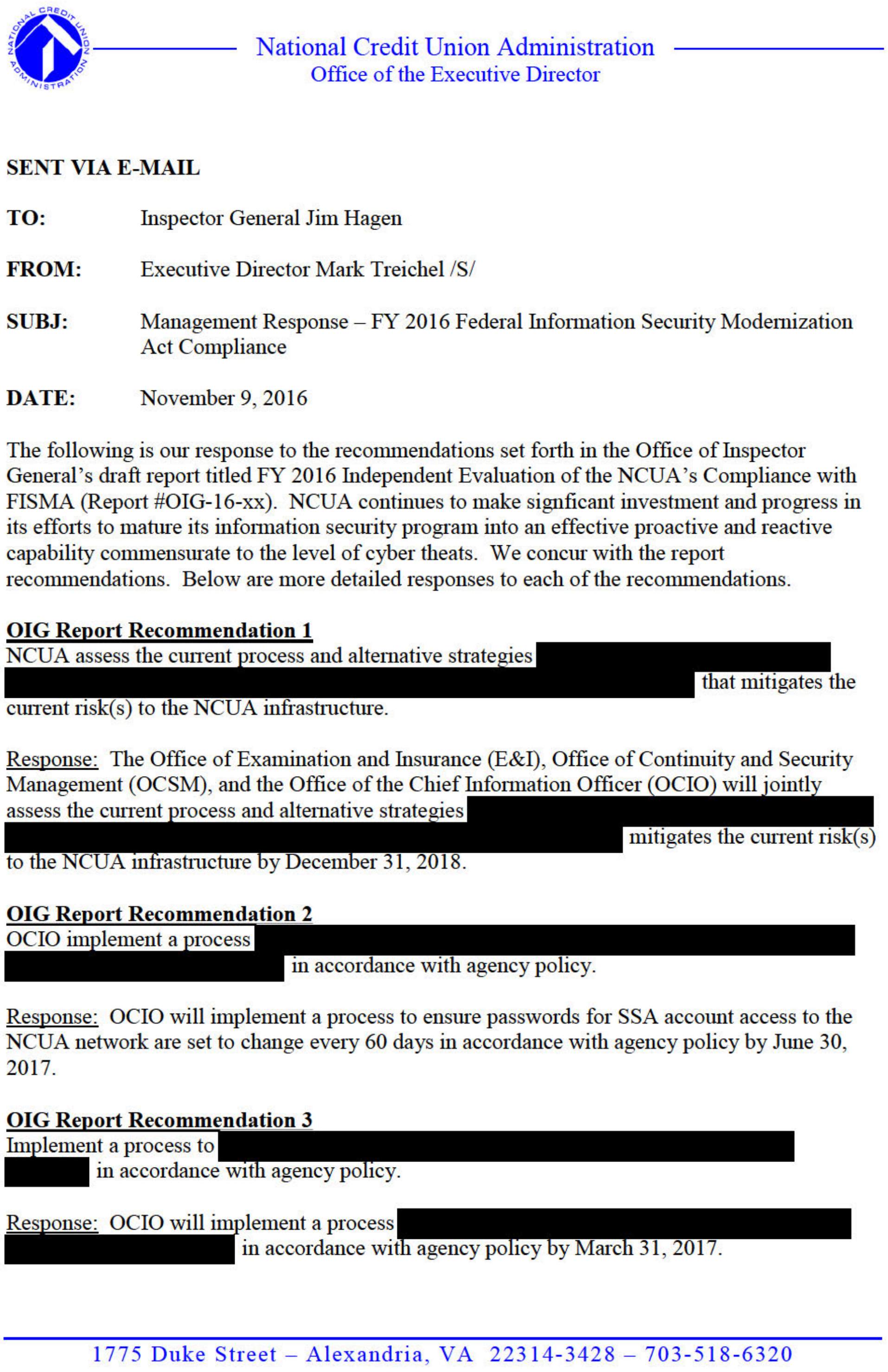
The purpose of a fully and formally documented Privacy Program is to define the agency-wide privacy policies and practices. Implementing comprehensive privacy policies and procedures mitigates the likelihood that NCUA staff members will not fully address privacy throughout the lifecycle of the agency's information systems. In addition, formal privacy policies and procedures will provide employees and contractors with consistent and comprehensive guidance to adequately handle and protect agency and credit union PII. Furthermore, these policies and procedures will facilitate accountability in effectively administering the implementation and management of the agency's Privacy Program. Consequently, these formal policies and procedures will help NCUA ensure proper handling of PII, ultimately mitigating the potential for personal harm, loss of public trust, or increased costs associated with inappropriate or unauthorized access to PII.

Once NCUA finalizes and implements its privacy program, OCIO will be able to incorporate NCUA"s privacy controls into the General Support System security plan.

Recommendations:

We are not making additional recommendations at this time.

Appendix A: NCUA Management Response



National Credit Union Administration
Office of the Executive Director

SENT VIA E-MAIL

TO: Inspector General Jim Hagen

FROM: Executive Director Mark Treichel /S/

SUBJ: Management Response – FY 2016 Federal Information Security Modernization Act Compliance

DATE: November 9, 2016

The following is our response to the recommendations set forth in the Office of Inspector General's draft report titled FY 2016 Independent Evaluation of the NCUA's Compliance with FISMA (Report #OIG-16-xx). NCUA continues to make signficant investment and progress in its efforts to mature its information security program into an effective proactive and reactive capability commensurate to the level of cyber theats. We concur with the report recommendations. Below are more detailed responses to each of the recommendations.

OIG Report Recommendation 1
NCUA assess the current process and alternative strategies [redacted] that mitigates the current risk(s) to the NCUA infrastructure.

Response: The Office of Examination and Insurance (E&I), Office of Continuity and Security Management (OCSM), and the Office of the Chief Information Officer (OCIO) will jointly assess the current process and alternative strategies [redacted] mitigates the current risk(s) to the NCUA infrastructure by December 31, 2018.

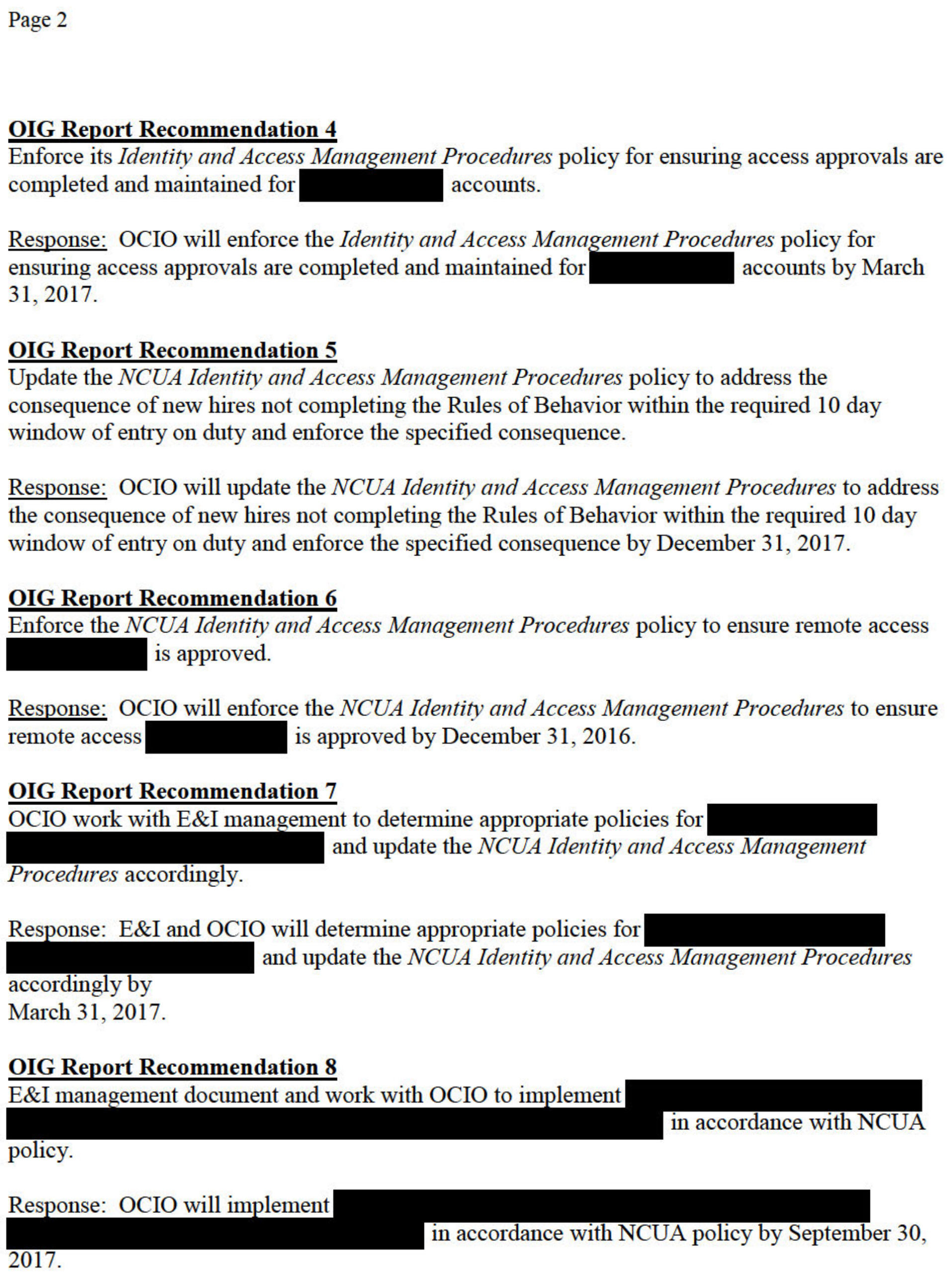
OIG Report Recommendation 2
OCIO implement a process [redacted] in accordance with agency policy.

Response: OCIO will implement a process to ensure passwords for SSA account access to the NCUA network are set to change every 60 days in accordance with agency policy by June 30, 2017.

OIG Report Recommendation 3
Implement a process to [redacted] in accordance with agency policy.

Response: OCIO will implement a process [redacted] in accordance with agency policy by March 31, 2017.

1775 Duke Street – Alexandria, VA 22314-3428 – 703-518-6320



Page 2

OIG Report Recommendation 4
Enforce its *Identity and Access Management Procedures* policy for ensuring access approvals are completed and maintained for [redacted] accounts.

Response: OCIO will enforce the *Identity and Access Management Procedures* policy for ensuring access approvals are completed and maintained for [redacted] accounts by March 31, 2017.

OIG Report Recommendation 5
Update the *NCUA Identity and Access Management Procedures* policy to address the consequence of new hires not completing the Rules of Behavior within the required 10 day window of entry on duty and enforce the specified consequence.

Response: OCIO will update the *NCUA Identity and Access Management Procedures* to address the consequence of new hires not completing the Rules of Behavior within the required 10 day window of entry on duty and enforce the specified consequence by December 31, 2017.

OIG Report Recommendation 6
Enforce the *NCUA Identity and Access Management Procedures* policy to ensure remote access [redacted] is approved.

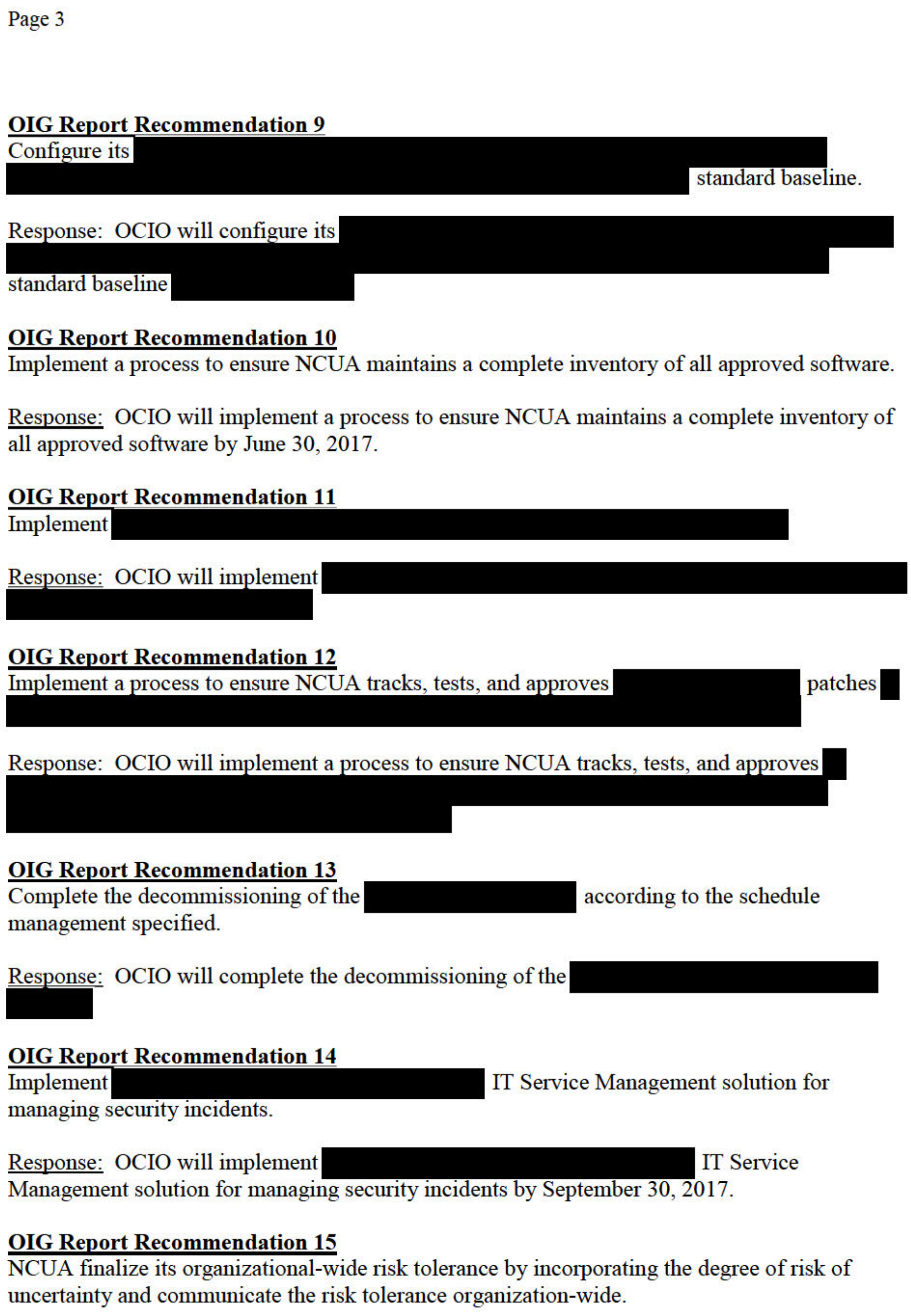
Response: OCIO will enforce the *NCUA Identity and Access Management Procedures* to ensure remote access [redacted] is approved by December 31, 2016.

OIG Report Recommendation 7
OCIO work with E&I management to determine appropriate policies for [redacted] and update the *NCUA Identity and Access Management Procedures* accordingly.

Response: E&I and OCIO will determine appropriate policies for [redacted] and update the *NCUA Identity and Access Management Procedures* accordingly by
March 31, 2017.

OIG Report Recommendation 8
E&I management document and work with OCIO to implement [redacted] in accordance with NCUA policy.

Response: OCIO will implement [redacted] in accordance with NCUA policy by September 30, 2017.



Page 3

OIG Report Recommendation 9
Configure its [redacted] standard baseline.

Response: OCIO will configure its [redacted] standard baseline [redacted]

OIG Report Recommendation 10
Implement a process to ensure NCUA maintains a complete inventory of all approved software.

Response: OCIO will implement a process to ensure NCUA maintains a complete inventory of all approved software by June 30, 2017.

OIG Report Recommendation 11
Implement [redacted]

Response: OCIO will implement [redacted]

OIG Report Recommendation 12
Implement a process to ensure NCUA tracks, tests, and approves [redacted] patches [redacted]

Response: OCIO will implement a process to ensure NCUA tracks, tests, and approves [redacted]

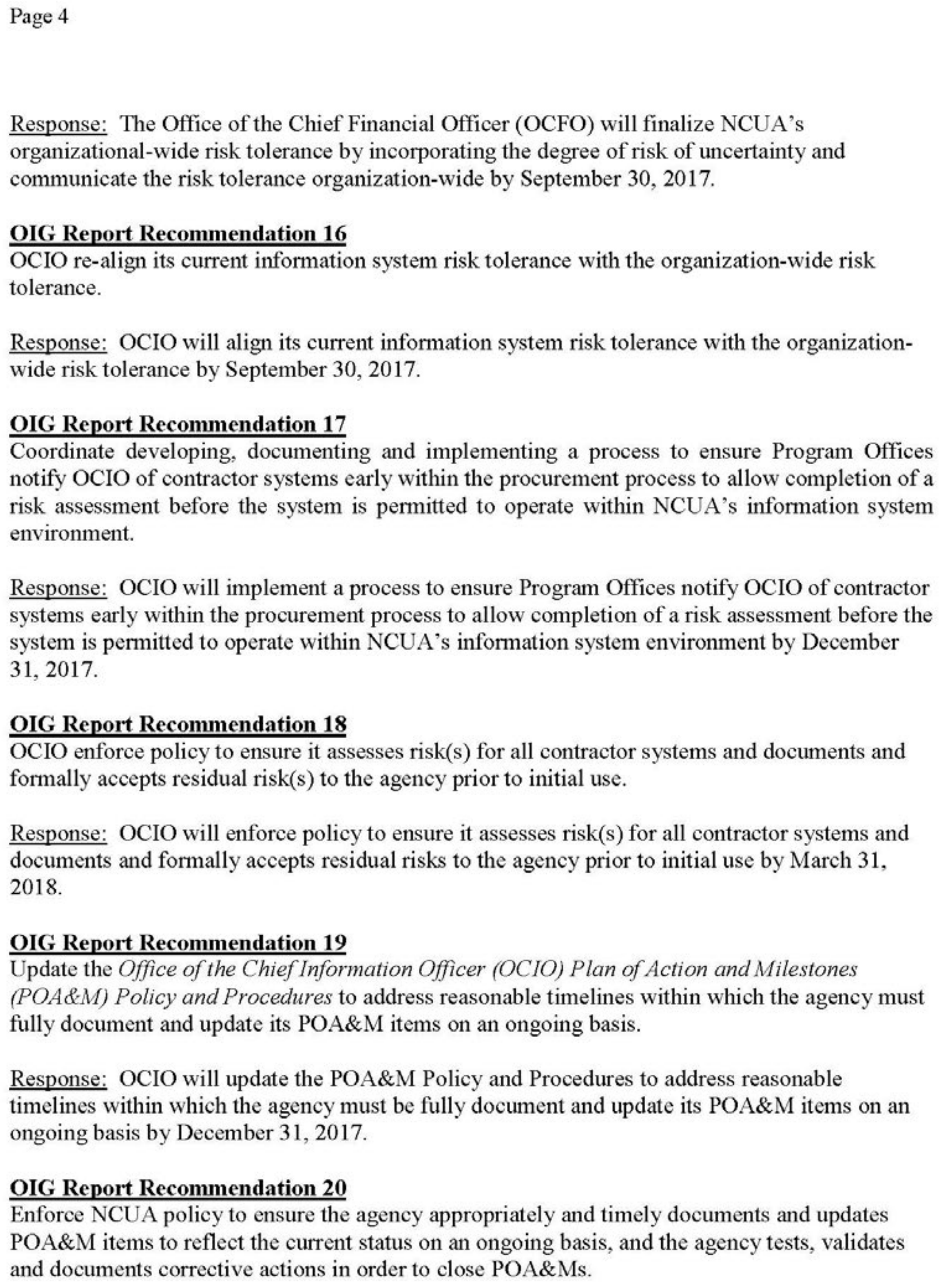
OIG Report Recommendation 13
Complete the decommissioning of the [redacted] according to the schedule management specified.

Response: OCIO will complete the decommissioning of the [redacted]

OIG Report Recommendation 14
Implement [redacted] IT Service Management solution for managing security incidents.

Response: OCIO will implement [redacted] IT Service Management solution for managing security incidents by September 30, 2017.

OIG Report Recommendation 15
NCUA finalize its organizational-wide risk tolerance by incorporating the degree of risk of uncertainty and communicate the risk tolerance organization-wide.



Page 4

Response: The Office of the Chief Financial Officer (OCFO) will finalize NCUA's organizational-wide risk tolerance by incorporating the degree of risk of uncertainty and communicate the risk tolerance organization-wide by September 30, 2017.

OIG Report Recommendation 16
OCIO re-align its current information system risk tolerance with the organization-wide risk tolerance.

Response: OCIO will align its current information system risk tolerance with the organization-wide risk tolerance by September 30, 2017.

OIG Report Recommendation 17
Coordinate developing, documenting and implementing a process to ensure Program Offices notify OCIO of contractor systems early within the procurement process to allow completion of a risk assessment before the system is permitted to operate within NCUA's information system environment.

Response: OCIO will implement a process to ensure Program Offices notify OCIO of contractor systems early within the procurement process to allow completion of a risk assessment before the system is permitted to operate within NCUA's information system environment by December 31, 2017.

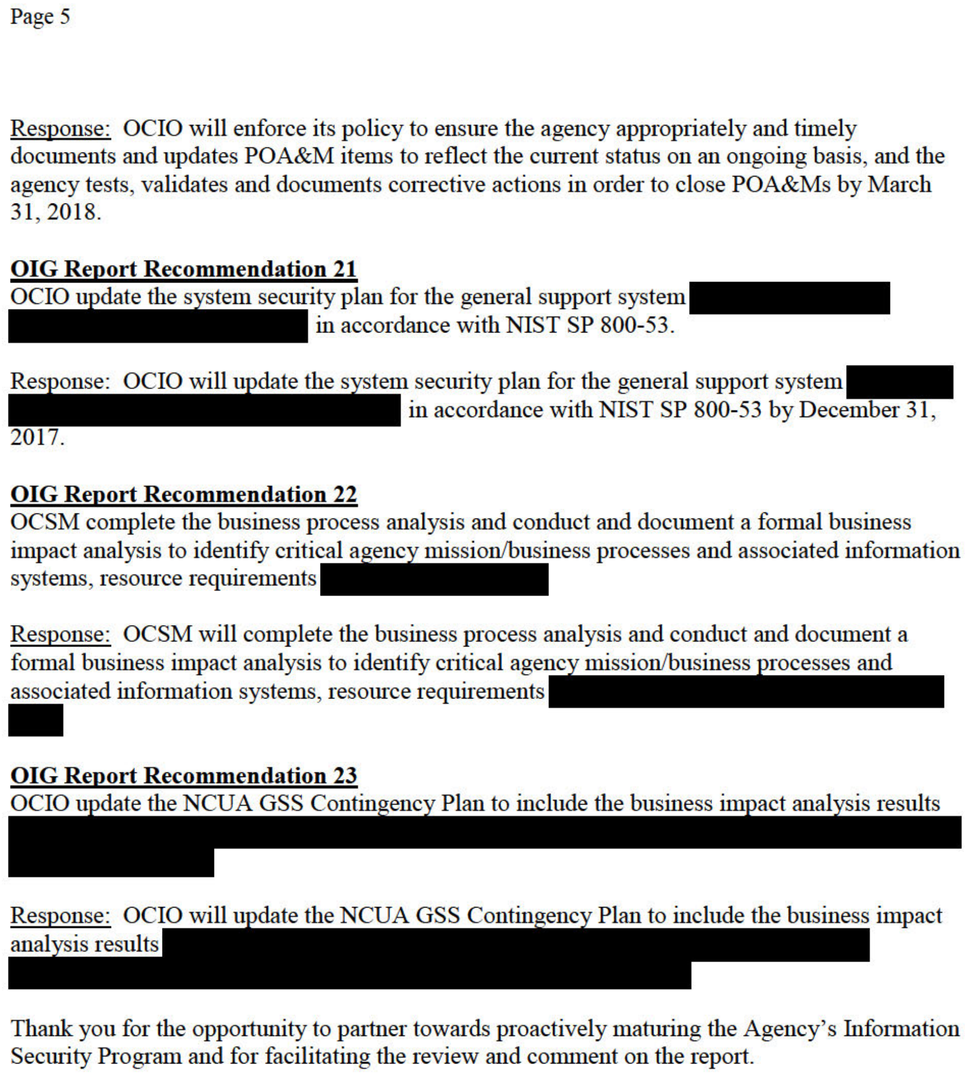
OIG Report Recommendation 18
OCIO enforce policy to ensure it assesses risk(s) for all contractor systems and documents and formally accepts residual risk(s) to the agency prior to initial use.

Response: OCIO will enforce policy to ensure it assesses risk(s) for all contractor systems and documents and formally accepts residual risks to the agency prior to initial use by March 31, 2018.

OIG Report Recommendation 19
Update the *Office of the Chief Information Officer (OCIO) Plan of Action and Milestones (POA&M) Policy and Procedures* to address reasonable timelines within which the agency must fully document and update its POA&M items on an ongoing basis.

Response: OCIO will update the POA&M Policy and Procedures to address reasonable timelines within which the agency must be fully document and update its POA&M items on an ongoing basis by December 31, 2017.

OIG Report Recommendation 20
Enforce NCUA policy to ensure the agency appropriately and timely documents and updates POA&M items to reflect the current status on an ongoing basis, and the agency tests, validates and documents corrective actions in order to close POA&Ms.



Page 5

Response: OCIO will enforce its policy to ensure the agency appropriately and timely documents and updates POA&M items to reflect the current status on an ongoing basis, and the agency tests, validates and documents corrective actions in order to close POA&Ms by March 31, 2018.

OIG Report Recommendation 21
OCIO update the system security plan for the general support system [redacted] in accordance with NIST SP 800-53.

Response: OCIO will update the system security plan for the general support system [redacted] in accordance with NIST SP 800-53 by December 31, 2017.

OIG Report Recommendation 22
OCSM complete the business process analysis and conduct and document a formal business impact analysis to identify critical agency mission/business processes and associated information systems, resource requirements [redacted]

Response: OCSM will complete the business process analysis and conduct and document a formal business impact analysis to identify critical agency mission/business processes and associated information systems, resource requirements [redacted]

OIG Report Recommendation 23
OCIO update the NCUA GSS Contingency Plan to include the business impact analysis results [redacted]

Response: OCIO will update the NCUA GSS Contingency Plan to include the business impact analysis results [redacted]

Thank you for the opportunity to partner towards proactively maturing the Agency's Information Security Program and for facilitating the review and comment on the report.

Appendix B: Acronyms and Abbreviations

AMAC	Asset Management and Assistance Center
ATO	Authority To Operate
BIA	Business Impact Analysis
BPA	Business Process Analysis
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CLA	CliftonLarsenAllen, LLP
COOP	Continuity Of Operations Program
CPO	Chief Privacy Officer
CUSO	Credit Union Service Organization
DCIO	Deputy Chief Information Officer
DHS	Department of Homeland Security
DISA	Defense Information Systems Agency
EComp	Employees Compensation Operations and Management Portal
EEO	Equal Employment Opportunity
eOPF	Electronic Official Personnel Folder
ESS	Electronic Security System
FDCC	Federal Desktop Core Configuration
FISMA	Federal Information Security Management Act
FISMA 2014	Federal Information Security Modernization Act
FY	Fiscal Year
GISRA	Government Information Security Reform Act of 2002
HSPD	Homeland Security Presidential Directive

ID	Identification
IDS	Intrusion Detection System
IT	Information Technology
MARS	Management Automated Resource System
MDP	Management Development Program
MEF	Mission Essential Functions
NCUA	National Credit Union Administration
NIST	National Institute of Standards and Technology
OCIO	Office of the Chief Information Officer
OCSM	Office of Continuity and Security Management
OIG	Office of Inspector General
OMB	Office of Management and Budget
PII	Personally Identifiable Information
PIV	Personal Identity Verification
POA&M	Plan Of Action and Milestones
RA	Reasonable Accommodation
SAOP	Senior Agency Official for Privacy
SQL	Structured Query Language
SSA	State Supervisory Authority
STIG	Security Technical Implementation Guide
USGCB	United States Government Configuration Baseline
VPN	Virtual Private Network