CORPORATION FOR NATIONAL & COMMUNITY SERVICE

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2017 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG Report 18-03

Prepared by:

CliftonLarsonAllen LLP
901 North
Glebe Road, Suite 200
Arlington, VA 22203

This report was issued to Corporation management on December 18, 2017. Under the laws and regulations governing audit follow up, the Corporation is to make final management decisions on the report's findings and recommendations no later than June 18, 2018, and complete its corrective actions by December 18, 2018. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

OFFICE OF INSPECTOR GENERAL
CORPORATION FOR
NATIONAL & COMMUNITY SERVICE

December 18, 2017

TO: Jeffrey Page
Chief Operating Officer

Tom Hanley
Chief Information Officer

FROM: Stuart Axenfeld /s/
Assistant Inspector General for Audit

SUBJECT: Fiscal Year 2017 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service (OIG Report 18-03)

Attached is the final report on the Office of Inspector General's (OIG) Report 18-03, Fiscal Year 2017 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service. This evaluation was performed by CliftonLarsonAllen LLP in accordance with the Quality Standards for Inspections and Evaluations promulgated by the Council of Inspectors General on Integrity and Efficiency (CIGIE).

Under the Corporation's audit resolution policy, a final management decision on the findings and recommendations in this report is due by June 18, 2018. Notice of final action is due by December 18, 2018.

Should you have any questions about this report, please contact Guy Hadsall, Chief Technology Officer, at 202-606-9375; Thomas Chin, Audit Manager, at 202-606-9362; or me at 202-606-9360.

Attachment

cc: Lori Giblin, Chief Risk Officer
Robert McCarty, Chief Financial Officer
Andrea Simpson, Chief Information Security Officer
Edward Davis, Deputy Chief Information Officer
Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

CliftonLarsonAllen

Fiscal Year 2017 Federal Information Security Modernization Act Evaluation for the Corporation for National and Community Service

December 18, 2017

Final Report

CliftonLarsonAllen

CliftonLarsonAllen LLP
901 North Glebe Road, Suite 200
Arlington, VA 22203

571-227-9500 | fax 571-227-9552

CLAconnect.com

December 18, 2017

Kim Mansaray, Acting Chief Executive Officer
Corporation for National and Community Service
250 E Street, Suite 1400, SW
Washington, D.C. 20525

Dear Ms. Mansaray:

The Corporation for National and Community Service (CNCS or the Corporation) has devoted significant resources to improving its information security over the past few years, with meaningful progress. Its information security program is approaching effectiveness, though it is not sufficiently mature. With continued effort and investment, CNCS can reach that milestone in the near future.

Doing so requires that CNCS address the new and continuing weaknesses identified in our evaluation, which pose significant risks to information security and privacy. At the completion of our fieldwork, CNCS had not completed corrective actions for eight prior recommendations, four of which date back to FY 2014. We found inadequate risk management, configuration management, identity and access management, information security continuous monitoring, and contingency planning. Enforcement of information security is inconsistent across the enterprise, with field components remaining especially vulnerable.

The FISMA evaluation requires us to assess the maturity of five function areas in CNCS's information security program. This assessment used objective metrics that are standardized across the Federal government. To be considered effective, an agency's IT security must be rated *Managed and Measurable* (Level 4), on a five-point scale from *Ad hoc* (Level 1) to *Optimized* (Level 5). CNCS did not reach that level. Four of the five function areas at CNCS achieved a maturity level of *Defined* (Level 2). One function area, *Respond*, was found to be *Consistently Implemented* (Level 3).

FISMA evaluators are also permitted to rate judgmentally the effectiveness of seven components (“domains”) of a Cybersecurity Framework established by National Institute of Standards and Technology (NIST). CNCS's cybersecurity was not effective in five of these domains: risk management, configuration management, identity and access management, information security continuous monitoring, and security planning. The remaining domains, security training and incident response, were determined to be effective. Nevertheless, we recognize that there has been progress over prior year assessments and that CNCS's information security is closer to effectiveness.

Considering both these subjective and objective results, we conclude that information security at CNCS has not yet achieved an effective level. The findings set forth in the attached report reflect continuing vulnerabilities in information security, which leave CNCS operations and assets at risk of unauthorized access, misuse and disruption. This report offers 34 new or modified recommendations to assist CNCS in strengthening its information security program. Eight of these relate to prior findings that have not been completely addressed by CNCS.

The CNCS Office of Inspector General (CNCS-OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to evaluate the Corporation's compliance with the Federal Information Security Modernization Act of 2014 (FISMA) for Fiscal Year 2017. CLA's report is enclosed.

The objective of this evaluation was to assess the effectiveness of CNCS's information security program in accordance with FISMA, Office of Management and Budget (OMB) requirements, and NIST guidance. Our evaluation was performed in accordance with the *Quality Standards for Inspection and Evaluation*, issued by the Council of Inspectors General on Integrity and Efficiency. In addition, the evaluation included inquiries, observations, inspection of documents and records, and testing of controls.

The evaluation included the testing of selected management, technical, and operational controls outlined in NIST Special Publication 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for the following information systems:

- General Support System (GSS)
- Electronic-Systems for Program Agreements and National Service Participants (eSPAN)
- My AmeriCorps Portal (a subsystem of eSPAN)
- Momentum Financial Management System

We appreciate the assistance we received from CNCS and appreciate the opportunity to serve you. We will be pleased to discuss any questions or concerns you may have regarding the contents of this report.

Very truly yours,

CliftonLarsonAllen LLP

CLIFTONLARSONALLEN LLP

TABLE OF CONTENTS

BACKGROUND

Corporation Overview

The Corporation for National and Community Service (CNCS or the Corporation) was established in 1993 to connect Americans of all ages and backgrounds with opportunities to give back to their communities and the nation. Its mission is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. The Corporation's Board of Directors and Chief Executive Officer (CEO) are appointed by the President and confirmed by the Senate. The CEO oversees the agency, which employs approximately 620 employees operating throughout the United States and its territories. The Board of Directors sets broad policies and direction for the Corporation and oversees actions taken by the CEO with respect to standards, policies, procedures, programs, and initiatives necessary to carry out the mission of the Corporation.

Information Technology Overview

CNCS relies on information technology (IT) systems to accomplish its mission of providing and managing volunteer services nationally. The Corporation has a Federal Information Security Modernization Act (FISMA) inventory of six information systems – the Network or General Support System (GSS), Electronic-Systems for Program Agreements and National Service Participants (eSPAN) (which includes the eGrants grants management system), Momentum, AmeriCorps Health Benefits, AmeriCorps Childcare Benefits System, and public websites. The Federal Information Processing Standard (FIPS) Publication (PUB) 199[1] security categorization levels of these systems are moderate (five of six systems) and low (Public Website). All six systems are hosted and operated by third-party service providers, although the Corporation also hosts certain components of the GSS. The Corporation's network consists of multiple sites: Headquarters (HQ), one Field Financial Management Center (FFMC), five National Civilian Community Corps (NCCC) campuses, one Volunteers in Service to America (VISTA) Member Support Unit (VMSU), and more than 50 AmeriCorps state offices throughout the United States. These facilities are connected with commercially managed high-speed network connections.

To balance high levels of service and reduce costs, CNCS's Office of Information Technology (OIT) has outsourced the operation, maintenance and support of most of the Corporation's IT systems. While outsourcing is not inherently detrimental to the security posture of an organization, it introduces different considerations and new risks regarding the protection of information and information systems. Despite this outsourcing, CNCS by law retains responsibility for complying with the requirements of the FISMA and security control implementation.

[1] Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides guidance determining the security category (i.e., low, moderate, high) of federal information systems based on confidentiality, integrity and availability.

Consequently, CNCS and its contractors share responsibility for managing the following three primary information systems:

- **GSS** – Primary network services for CNCS, including related peripherals, telecommunications equipment, and collaboration services. It also provides office automation support for e-mail, Voice & Video Services (Voice over Internet Protocol), commercial software applications, wireless (CNCS and CNCS-Guest networks), and communications services for several CNCS created, owned, and maintained applications. The CNCS GSS networks facilitate data transmission to Momentum, the Department of Agriculture (National Finance Center), CNCS public websites, and Department of Treasury.

- **Momentum Financial Management System** – Momentum is the official system of record for financial management at CNCS. Momentum records financial transactions including purchasing, accounts receivable, accounts payable, disbursements (to include payroll), and budget activities. Momentum also provides CNCS the functions needed to produce and provide financial reports and internal controls.

- **Electronic-Systems for Program Agreements and National Service Participants (eSPAN)** - Maintains records on AmeriCorps members, terms of service, education awards, and payments. The eSPAN system uses electronic file transfers to receive enrollment data from the My AmeriCorps Portal, and to provide updated financial information to the National Service Trust. It is operated on behalf of CNCS under contract with ITCON Services LLC, which also manages the data warehouse for the My AmeriCorps Portal. My AmeriCorps Portal is a major web-based application under CNCS's network used to communicate AmeriCorps member enrollment and service completion data to the National Service Trust. The eGrants system, a sub-system of eSPAN incorporates all phases of grant making: applying, awarding, monitoring, reporting, and close out. eGrants also interfaces with Momentum and through Momentum to the Department of Health and Human Services' Payment Management System.

The Corporation's OIT provides support for the Corporation's technology and information needs, as well as project management services during the life cycle of major system acquisitions through daily operations. The Chief Information Officer (CIO) leads the OIT and the overall Corporation's IT operations. The CIO is assisted by the Chief Information Security Officer (CISO), who manages the OIT/Cybersecurity office responsible for computer security and privacy issues and addressing statutory requirements of an organization-wide information security program.

CNCS establishes specific organization-defined IT security policies, procedures, and parameters in its Cybersecurity Controls Family document, which incorporates the National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*.

FISMA Legislation

The Federal Information Security Modernization Act of 2014[2] (FISMA) provides a comprehensive framework for ensuring effective security controls over information resources supporting Federal operations and assets. FISMA requires federal agencies to develop, document, and implement an agency wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source.

The statute also provides a mechanism for improved oversight of Federal agency information security programs. FISMA requires agency heads to ensure that (1) employees are sufficiently trained in their security responsibilities, (2) security incident response capability is established, and (3) information security management processes are integrated with the agency's strategic and operational planning processes. All agencies must also report annually to the Office of Management and Budget (OMB) and to congressional committees on the effectiveness of their information security program.

Federal agencies are to provide information security protections commensurate with the risk and magnitude of the harm resulting from unauthorized access, use, disclosure, disruption, modification, or destruction of information collected or maintained by the agency. As specified in FISMA, the agency CIO or senior official is responsible for overseeing the development and maintenance of security operations that continuously monitor and evaluate risks and threats.

FISMA also requires agency Inspectors Generals (IGs) to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the Federal Information Processing Standards to establish agency baseline security requirements.

FY 2017 IG FISMA Reporting Metrics

OMB and the Department of Homeland Security (DHS) annually provide instructions to Federal agencies and Inspectors General for preparing FISMA reports. In November 2016, OMB issued Memorandum M-17-05, *Fiscal Year 2016-2017 Guidance on Federal Information Security and Privacy Management Requirements*. The memorandum establishes information security priorities, and provides agencies with FY 2016-2017 FISMA and Privacy Management reporting guidance and deadlines. Accordingly, the *FY 2017 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics,* provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.

[2] The Federal Information Security Modernization Act of 2014 (Public Law 113–283—December 18, 2014) amends the Federal Information Security Management Act of 2002 to: (1) reestablish the oversight authority of the Director of the Office of Management and Budget (OMB) with respect to agency information security policies and practices and (2) set forth authority for the Secretary of the Department of Homeland Security to administer the implementation of such policies and practices for information systems.

The FY 2017 metrics are based on a maturity model approach begun in prior years and align the metrics with all five function areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond, and Recover. The Cybersecurity Framework (CSF) provides agencies with a common structure for identifying and managing cybersecurity agency-wide risks across the enterprise IT and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 1**.

Table 1: Aligning the Cybersecurity Framework Security Functions to the FY 2017 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2017 IG FISMA Metric Domains
Identify	Risk Management and Contractor Systems
Protect	Configuration Management, Identity and Access Management, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

The foundational levels of the maturity model spectrum focus on the development of sound, risk-based policies and procedures, while the advanced levels capture the institutionalization and effectiveness of those policies and procedures. **Table 2** explains the five maturity model levels. A function information security area is not considered effective unless it achieves a rating of Level 4, *Managed and Measurable*. This is the first year in which the complete maturity model, with its objective scoring, has been available.

Table 2: IG Assessment Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad hoc	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategy are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Evaluation methodology and requirements

The CNCS Office of Inspector General (CNCS-OIG) engaged CliftonLarsonAllen LLP to conduct the required evaluation of CNCS's information security program and practices. The objective of this evaluation was to assess the effectiveness of CNCS's information security program in accordance with FISMA, OMB requirements, and NIST guidance.

Our evaluation was performed in accordance with the *Quality Standards for Inspection and Evaluation* issued by the Council of Inspectors General on Integrity and Efficiency. In addition, the evaluation included inquiries, observations, inspection of documents and records, and testing of controls.

For this evaluation, we reviewed selected management, operational, and technical controls in accordance with NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*. Our evaluation included an assessment of information security controls both at the enterprise and at the facility levels (selected NCCC campuses and State Offices). In addition, our evaluation included an assessment of effectiveness for each of the seven FY 2017 IG FISMA Metric Domains and the maturity level of the five Cybersecurity Framework Security Functions. See Appendix I for the detailed scope and methodology.

SUMMARY OF RESULTS

Progress since FY 2016

CNCS continues to improve its information security and privacy program and its compliance with FISMA, OMB requirements, and applicable NIST guidance. Specifically, it closed 19 out of 27 open recommendations from the FY 2014 – FY 2016 FISMA evaluations.[3] Further, the Corporation has made improvements in the following areas:

- Establishment of security assessment standards to promote consistency and quality.
- Development of business impact assessments for each critical system with participation from the business owners.
- Implementation of the United States Government Configuration Baseline (USGCB) for desktops, and monitored for compliance with those approved settings.
- Implementation of a process to monitor data backup failures.

As of the close of our fieldwork, however, CNCS had not completed corrective actions for eight prior recommendations. Four of these date back to the FY 2014 FISMA evaluation.

Current results

Despite the noted progress, CNCS must make additional improvements to achieve effective information security. Weaknesses identified in this evaluation include inconsistent enforcement of information security policies and ineffective communication between CNCS management and the individual field offices. At the sampled NCCC campuses and State Offices, we found multiple weaknesses in the areas of vulnerability and patch management, access controls for mobile devices, audit logging, and physical inventory management. OIT exercises less responsibility and oversight of field locations than it does for IT at the Corporation's headquarters.

Our conclusions as to the effectiveness of CNCS's IT security incorporate multiple sets of results, set forth below.

1. <u>FISMA maturity scores and judgmental assessment</u>

FISMA requires evaluators across the Federal government to respond to 61 objective questions, from which a DHS algorithm calculates a maturity score for each of five function areas. As set forth in the chart below, CNCS was rated at maturity level 2, *Defined*, in four of the five areas, and at level 3, *Consistently Implemented*, in one area.[4] Thus, by these objective metrics, CNCS fell below the specified threshold of effectiveness, which is level 4, *Managed and Measurable*.

[3] The prior FISMA evaluations were performed by another CPA firm.

[4] The most frequent maturity level rating across the Protect function served as the overall Protect function rating.

An evaluator may also make a subjective, judgmental assessment of the effectiveness of an agency's IT security in each of seven metric domains. This opportunity allows the evaluation to reflect information that may not be captured by the objective assessment. Our subjective assessment concluded that CNCS's IT security was effective in the areas of security training and incident response, above the level indicated by the maturity model. In the remaining areas, we determined that CNCS has made progress over past years and is approaching effectiveness.

Table 3 below summarizes the maturity scores and judgmental results by category.

Table 3: FY 2017 IG Cybersecurity Framework Domain Ratings

Cybersecurity Framework Security Functions[5]	Metric Domains	Calculated Maturity Level	Independent Assessor Evaluation
Identify	**Risk Management**	Defined (Level 2)	Not Effective
Protect	**Configuration Management**	Defined (Level 2)	Not Effective
Protect	**Identity and Access Management**	Defined (Level 2)	Not Effective
Protect	**Security Training**	Consistently Implemented (Level 3)	Effective
Detect	**Information Security Continuous Monitoring**	Defined (Level 2)	Not Effective
Respond	**Incident Response**	Consistently Implemented (Level 3)	Effective
Recover	**Contingency Planning**	Defined (Level 2)	Not Effective

2. Detailed findings

Table 4 below summarizes our detailed findings. We have separated them into enterprise-level findings—those pertaining to control weaknesses at CNCS Headquarters in Washington, DC—and facility-level findings—relating to control weaknesses discovered at the Vicksburg, Mississippi and Denver, Colorado NCCC campuses and Jackson, Mississippi and Denver Colorado State Offices.

[5] See Table 1 and Table 2 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

Table 4: Findings Noted During the FY 2017 FISMA Evaluation of CNCS

IG FISMA Metric Domain	Enterprise Level Findings	Facility Level Findings
Risk Management	Expired system authorization to operate (Finding 1)	Unpatched and unsupported software (Finding 9)
	Incomplete system security plans (Finding 1)	Incomplete and inaccurate information technology asset inventory (Finding 13)
	Inadequate system risk assessments (Finding 1)	Inadequate physical and environmental controls (Finding 14)
	Undocumented Plans of Action and Milestones (PO&AMs) (Finding 1)	
	Incomplete enterprise risk management strategy (Finding 1)	
	Inconsistent enforcement of an agency-wide information security program across the enterprise (Finding 8)	
	Incomplete and inaccurate information technology asset inventory	
Configuration Management	Configuration baselines not fully implemented (Finding 2)	
	Incomplete or undocumented system change testing (Finding 2)	
Identity and Access Management	Inadequate account management controls (Finding 3)	Unsecured mobile devices (Finding 10)
	Lack of multifactor authentication (Finding 4)	Inadequate monitoring of wireless access connections (Finding 11)
	Insufficient personnel screening process (Finding 6)	Inadequate protection of personally identifiable information (Finding 12)
Information Security Continuous Monitoring	Inadequate review and analysis of audit logs (Finding 5)	
Contingency Planning	Inadequate disaster recovery test results analysis (Finding 7)	
	Incomplete Continuity of Operations Plan (COOP) (Finding 7)	

Overall, we conclude that information security at CNCS has improved in a number of areas. With continued effort, attention and investment, especially to achieve greater consistency across the enterprise, the information security program will mature and can cross the effectiveness threshold in the near future. At present, however, the weaknesses that we identified leave CNCS operations and assets at risk of unauthorized access, misuse and disruption.

To address these weaknesses, we offer 34 new or modified recommendations to assist CNCS in strengthening its information security program. Eight of these are related to prior findings that CNCS did not resolve completely.

Management Comments

In response to the draft report, CNCS accepted 10 recommendations, partially accepted 17 recommendations, and rejected the remaining 7 recommendations from the 34 recommendations.

In general, management's comments for the 17 partially accepted recommendations were to review the recommendations further to consider cost-effective alternative processes to address the concerns, determining if the recommendations align with the future direction of managing information security across the organization, and determining where improvements can be made using existing processes, tools and resources. This included CNCS only partially accepting the control weakness of running an open unmonitored (i.e., no passwords, no restrictions) wireless access network at one of its field locations. CNCS rejected seven recommendations because it stated that it already had processes in place to address the recommendations. However, as our test results indicated, we noted control weaknesses in the implementation of CNCS policies and procedures and accordingly we made recommendations to improve current processes or implement improvements to existing policies and procedures. For the ten accepted recommendations, management stated that an open corrective action plan is in place to address the recommendations, it will incorporate the recommendations into existing processes, or CNCS is actively working on the recommendations. CNCS did not provide a timeline for implementation of the recommendations. The Corporation indicated that it will continue to use the Plan of Actions and Milestones (POA&M) as the process by which cybersecurity corrective actions are tracked and managed.

CNCS indicated that the FISMA evaluation failed to properly consider that a small agency like CNCS could not be held to the same level of maturity as large federal agencies and only a multi-year approach to CNCS's evaluation is meaningful. Management also stated that CNCS has devoted necessary resources to demonstrate a consistent level of improvement in Cybersecurity. Since FY 2014, CNCS spending on cybersecurity professional support has steadily increased. We noted that the CISO has three full-time employees and a matrixed team of contractors supporting the Corporation's information security program. In addition, each CNCS system has an Information System Security Officer assigned with the responsibility of ensuring appropriate operational security posture is maintained for their information system. Although CNCS has sufficient resources to achieve a more mature information security program, it has only made incremental improvements to reduce enterprise risk. A more programmatic approach by the CISO to prioritize its risk base-remediation activities should result in a more mature information security program. Additionally, CNCS staff and contractors that have cybersecurity roles should be held accountable for the remediation of control deficiencies and for ensuring that the appropriate security posture is maintained for its information systems.

CNCS also stated they do not believe the evaluation sufficiently reflects the improved status of its Cybersecurity program demonstrated by the FY 2017 IG FISMA Metrics. In 2015, OMB directed DHS and the IG community to improve upon its measurements. As a result, OMB, DHS, and the Council of the Inspectors General on Integrity and Efficiency developed the FY 2017 IG FISMA Reporting Metrics in consultation with the Federal Chief Information Officer Council to build on the work begun in FY 2015 and 2016, in order to move the IT assessments to a maturity model approach and align the metrics with all five function areas in the NIST Cybersecurity Framework (CSF). Although the FY 2017 IG FISMA Metrics included all eight of the CSF metric domains in the maturity model approach, the FY 2016 IG Metrics only included two of the domains in the five level maturity model. Therefore, comparing prior year IG FISMA Metrics results since FY 2015 is not valid. The FY 2018 IG FISMA Metrics have been published by OMB; these are consistent with the FY 2017 criterion which is expected to provide yearly comparisons. CNCS should look forward to the results of the FY 2018 IG FISMA evaluation to make measurement comparisons.

CNCS's comments are included in the entirety in Appendix III.

FISMA Evaluation Findings

Enterprise Level Findings

1. CNCS Must Strengthen its Organization-wide Information Security Program

Cybersecurity Framework Domain: *Identify*
FY 17 FISMA IG Metric Area: *Risk Management*

FISMA requires agencies to develop, document and implement an agency-wide information security program to provide information security for the information and information systems that support the agency's operations. NIST SP 800-53, Revision 4, organization-wide information security program management (PM) controls place an emphasis on the overall security program and are intended to enable compliance with applicable federal laws, Executive Orders, directives, policies, regulations, and standards.

Our assessment found that CNCS has not properly implemented an organization-wide information security program. Specifically, we noted weaknesses in the following NIST SP 800-53 PM controls:

- Security Authorization Process
- Plan of Action and Milestones Process
- Risk Management Strategy

Security Authorization Process:
We noted deficiencies in the Corporation's security authorization process in the following areas:

- Authorization to Operate (ATO)
- System Security Plan (SSP)
- System Risk Assessment (RA)

NIST's Risk Management Framework (RMF) provides the structure for the security authorization of federal information systems. The process includes:

- Selecting and implementing security controls for the information system and describing how the controls are implemented in the system security plan;
- Assessing whether the controls are operating as intended;
- Analyzing and assessing risk to the information system based on weaknesses and vulnerabilities identified; and
- Authorizing the information system based on the determination of risk.

NIST SP 800-37, Revision 1, *Guide for Applying the Risk Management Framework to Federal Information Systems: A Security Life Cycle Approach*, provides guidelines for applying the RMF to Federal information systems.

Authorization to Operate

CNCS did not maintain current system authorizations to operate for all its information systems. Specifically, the eSPAN/My AmeriCorps Portal ATO expired on July 31, 2017 and management was not planning to issue a new ATO until December 2017. Therefore, the system is in operation without an ATO. The CISO specified that resources were prioritized on the new grants management system implementation project rather than security assessment and authorization activities for eSPAN. In addition, the CISO indicated that all other CNCS systems are currently under an ongoing ATO through the continuous monitoring program and eSPAN will be authorized in December 2017 under an ongoing ATO as well.

NIST SP 800-37 describes a security authorization as the “official management decision given by a senior organizational official to authorize operation of an information system and to explicitly accept the risk to organizational operations and assets, individuals, other organizations, and the Nation based on the implementation of an agreed-upon set of security controls.” “The security authorization package contains: (i) the security plan; (ii) the security assessment report; and (iii) the plan of action and milestones. The information in these key documents is used by authorizing officials to make risk-based authorization decisions.”

Without CNCS information systems authorized to operate, the Authorizing Official (AO) cannot be held accountable for accepting the risk to operate these systems. Further, the security posture of CNCS systems may not be at an acceptable level of risk to operate, and the Corporation may be exposed to unmitigated security risk, potentially compromising the Corporation’s information or information systems.

System Security Plans

The purpose of a system security plan is to describe the information system, including the system boundary, and document the security controls both planned and implemented for the system. The GSS, eSPAN and Momentum SSPs did not include the control implementation descriptions for the privacy controls,[6] including an indication of the common privacy controls and the implementation descriptions for the system specific privacy controls.

The FY 2016 FISMA evaluation report[7] noted a recommendation for the Corporation to update the SSPs to accurately describe the implementation details for the base NIST SP 800-53 security and privacy controls, and required control enhancements. Management indicated they took corrective action and closed the recommendation. However, we noted that although the implementation details for the base security controls and required control enhancements were included in the SSPs, the privacy controls were not documented. Management is still working on updating the system security plans to include the privacy control implementation descriptions.

NIST SP 800-37 requires the security plan, in addition to listing the security controls to be implemented, to describe the intended application of each control in the context of the information system with sufficient detail to enable a compliant implementation of the control.

[6] National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, Appendix J, includes privacy controls for federal agencies and information systems.

[7] FY14-FISMA-NFR 10, Recommendation 5, Part D, *Fiscal Year 2014 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 15-03, November 14, 2014).

Without documenting how the privacy controls are intended to be implemented for the Corporation's information systems, the CISO who is also assigned responsibility as the Chief Privacy Officer acting on behalf of the Senior Agency Official for Privacy (SAOP), and the system AO would not be able to validate compliance with the privacy controls.

System Risk Assessments:
A system risk assessment is performed to identify risks to the Corporation pertaining to the operation of CNCS's information systems. When assessing risk, an analysis of known threats and vulnerabilities should be considered. In addition, when agencies use systems owned and operated by external parties, it is necessary to ensure that external service providers employ adequate security controls in order to protect the agency's data.

CNCS did not adequately assess system risks. Specifically, we identified the following system risk assessments that did not consider all known system risks:

- The Security Assessment Report (risk assessment) for the GSS did not take into account assessed risk for the entire system environment. Specifically, the risk assessment conducted in February 2017 only addressed weaknesses identified for Microsoft Azure.[8] The risk assessment did not address control weaknesses for the other GSS components such as:
    - Networking equipment such as switches and firewalls located at Headquarters
    - CNCS Data Center and Backup Data Center
    - FasseTrack Inventory Control System, a single virtual machine running the SQL server
    - CNCS field offices connected to the Corporation Data Center

- The Security Assessment Report (risk assessment) for the Momentum application conducted in March 2017 did not address the following risk assessment elements as required by NIST:
    - Threat/vulnerability identification
    - Likelihood
    - Impact analysis
    - Risk determination
    - Control recommendation

In addition, information security risks to the Corporation from the use of the following external systems were not assessed:

- Department of Health and Human Services' Payment Management System
- General Service Administration, E2 Travel System
- Department of Agriculture, National Finance Center's Payroll System
- Department of Treasury, Bureau of Public Debt, WebTA System

For example, the CISO did not review the Service Organization Control Reports or risk assessments performed for these systems to gain an understanding of the information security risks identified, and assess and document the risks and impact to CNCS from the use of external systems.

[8] Azure is an Office 365 (O365) cloud computing-based subscription service offering from Microsoft. Services that CNCS is currently using that includes: Exchange Online, Lync Online, SharePoint Online and Mobile Phone Deployment.

The risk assessment weaknesses occurred because the CISO did not implement a process to ensure all known security risks to the GSS environment were integrated into the system risk assessments. In addition, management did not thoroughly review the Momentum risk assessment to ensure it encompassed all of the required risk assessment elements as specified by NIST. Lastly, the CIO and CISO indicated that due to using shared government resources that were authorized to operate by the individual federal agencies, CNCS did not take into account the risks associated with the use of these systems.

NIST SP 800-53, Revision 4, requires organizations to conduct an assessment of risk, including the likelihood and magnitude of harm, from the unauthorized access, use, disclosure, disruption, modification, or destruction of the information system and the information it processes, stores, or transmits. In addition, risk assessments should also take into account risk from external parties (e.g., service providers).

Without adequately documented risk assessments, the AO does not have the appropriate knowledge to ensure mitigation of known control weaknesses and make an informed risk-based decision on whether to authorize the system to operate. In addition, without assessing the risks associated with the use of external information systems, CNCS may not be aware of, and assess any risks to the Corporation inherent with the use of these systems.

Plan of Action and Milestones Process:
POA&Ms describe corrective action plans for system weaknesses noted from security control assessments, vulnerability assessments and system audits. The POA&Ms are used by the authorizing official to monitor the progress of remediation for system control weaknesses.

The POA&Ms for the GSS, Momentum and eSPAN did not include all known control weaknesses. Specifically, we noted the following related to POA&Ms:

- POA&Ms were not created for 12 controls from the GSS SSP that were documented as partially implemented and/or planned.
- POA&Ms were not created for any of the control weaknesses documented in the GSS Azure Security Assessment Report, dated February 13, 2017, Momentum Security Assessment Report, dated March 9, 2017 or the eSPAN Security Assessment Report, dated December 13, 2016. For example, control weaknesses identified included:
  - Secure baseline configurations were not defined. (GSS)
  - The configuration management process required updating to ensure that all new devices/services are scanned by Nessus and reviewed prior to being approved by the configuration management board. (GSS)
  - Security control assessments were not performed for Momentum on an annual basis as required by CNCS policy. Previous to the assessment performed in 2017, an assessment had not been performed since 2014. (Momentum)
  - An automated mechanism to integrate audit review, analysis, and reporting for the eSPAN Oracle logs was not implemented. (eSPAN)
  - The database recovery process was not tested to validate data could be retrieved should threat events occur. (eSPAN)

The CISO did not place the necessary attention to the POA&M management process to ensure all known control weaknesses were documented in the POA&Ms. For example, the Information System Security Officer (ISSO) was not accountable for confirming that POA&Ms were created for controls that were not yet implemented, and control weaknesses identified through the security control assessments. In addition, ongoing evaluations were not performed of the POA&Ms to validate that they included all known control weaknesses.

NIST SP 800-53, Revision 4, requires organizations to develop POA&Ms to document corrective action plans to remediate information system control weaknesses based on findings from security control assessments and continuous monitoring activities.

POA&Ms are used by the AO to evaluate corrective action plans and estimated timeframes for remediation of control weaknesses, and to monitor the progress of remediation. Without the completion of POA&Ms for known control weaknesses, a plan for corrective action is delayed, leaving CNCS susceptible to system security risks.

Risk Management Strategy:
CNCS did not complete the development, documentation and communication of an entity-wide program for managing risk associated with the operation and use of the Corporation's information systems in accordance with NIST standards. During FY 2017, a risk register was developed and submitted to the Risk Management Council for review and concurrence. In order to complete the entity-wide risk management program in accordance with NIST, CNCS needs to perform the following:

- Finalize the risk register.
- Establish the risk tolerance for the Corporation to include information security and privacy and communicate the risk tolerance throughout the organization.
- Develop, document and implement acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance.
- Develop, document and implement approaches for monitoring risk over time.

Once CNCS completes and communicates an organization-wide risk tolerance, OIT will need to align its strategic goals and requirements for protecting its information and information systems with the risk tolerance that supports the Corporation's mission. This will assist CNCS in managing risk associated with the operation and use of the Corporation's information systems.

A recommendation to document and fully implement a comprehensive and enterprise-wide risk management process was initially made in the FY 2014 FISMA evaluation.[9] Management indicated that corrective action had not been completed and the recommendation was not closed, with the scheduled completion date on March 31, 2018.

In April 2016, CNCS hired a Chief Risk Officer. As a result, the Corporation's organization-wide risk management strategy is in the early stages, beginning with identifying and categorizing organizational risks, and developing and communicating an organization-wide risk tolerance. This will enable the Office of Information Technology to align information system risk to the organization-wide risk tolerance.

[9] FY14-FISMA-NFR 4, Recommendation 1, *FY14 Federal Information Security Management Act (FISMA) Independent Evaluation for FY 2014* (OIG Report No. 15-03, November 14, 2014).

NIST requires organizations to develop an entity-wide program for managing risk associated with the operation and use of the agency's information systems. Specifically, NIST SP 800-53, Revision 4, states agencies 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; and implement the risk management strategy consistently across the organization."

NIST further states, "an organization-wide risk management strategy includes, for example, an unambiguous expression of 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."

Moreover, according to NIST, managing information system risks including system authorization decisions, should align with the organization-wide mission and risk tolerance:

NIST SP 800-37, Revision 1, specifies 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 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 organizational risks affecting mission/business success."

Without developing, documenting, and communicating an organization-wide risk strategy, information technology strategic goals, objectives and requirements for protecting information and information systems may not be aligned with the risk tolerance that supports CNCS's mission and business priorities. Ultimately, this will most likely lead to inconsistently managing and monitoring information security-related risks associated with the confidentiality, integrity and availability of the Corporation's information.

To assist CNCS in strengthening its organization-wide information security program, we recommend the Corporation:

> ***Recommendation 1:*** *Document and implement a process to ensure the Corporation's information systems under the continuous monitoring program are compliant with NIST requirements for ongoing authorizations. The process should include the requirement that the Information System Security Officers report to the CISO on the status of the conditions documented in the ATO, according to the required timelines. In addition, the CISO should ensure adequate resources are assigned to the security authorization process to ensure the ATO conditions are met. (New)*
>
> ***Recommendation 2:*** *Ensure the control implementation descriptions for the privacy controls are documented in the GSS, eSPAN and Momentum system security plans. (Modified Repeat)*

Recommendation 3: *Ensure that system risk assessments take into account all known risks associated with the operation and monitoring of the entire information system's environment, and include all risk assessment elements as required by NIST. System risk assessments should also consider risks associated with the reliance of security controls inherited from the GSS. (New)*

Recommendation 4: *Document and implement a process to assess and acknowledge the information security and privacy risks to the Corporation associated with the use of all external information systems. This can include reviews of the Service Organization Control reports or risk assessments performed for external systems to gain an understanding of the information security risks identified, and assess and document the risks to CNCS from the use of these systems. (New)*

Recommendation 5: *Document and implement a process to ensure all known control weaknesses for the Corporation's information systems are documented in the POA&Ms. This should include assigning responsibility to the Information System Security Officer to validate that POA&Ms are created for controls that are not yet implemented and control weaknesses identified through security control assessments, audits and other evaluations. (New)*

Recommendation 6: *Implement a process for the Chief Information Security Office to perform an ongoing evaluation of the POA&M management process to ensure all known control weaknesses were captured in the POA&Ms. (New)*

Recommendation 7: *Complete the development, documentation, and communication of an organization-wide risk management strategy associated with the operation and use of the Corporation's information systems in accordance with NIST standards. This should include:*

- *Finalizing the risk register*
- *Establishing the risk tolerance for the Corporation, including information security and privacy, and communicating the risk tolerance throughout the organization*
- *Developing, documenting, and implementing acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance*
- *Developing, documenting, and implementing approaches for monitoring risk over time (Modified Repeat)*

2. CNCS Needs to Improve its Configuration Management Controls

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Configuration Management*

The establishment and implementation of documented configuration management policies and procedures is essential to consistently implement security controls for the protection of Government systems and data. Policies and procedures establish expectations for how an agency and its contractors implement and maintain configuration management controls and become more important when contractors play a leading role in maintaining configuration baselines and tracking deviations.

We noted control weaknesses with the Corporation's configuration management program in the following areas:

- Standard Baseline Configurations
- System Change Controls

Standard Baseline Configurations:
Although CNCS implemented USGCB for desktops, and monitored for compliance with those approved settings, standard baseline configurations for all platforms in the CNCS information technology environment were not fully implemented. For example, standard baseline configurations have not been implemented for CNCS operating systems, databases, servers, network devices, VMware, and Web browsers. The CISO stated that the Center for Internet Security (CIS) benchmarks have been selected as the standard baseline configurations and they were in the process of implementing the baselines.

The FY 2016 FISMA evaluation noted recommendations related to baseline configurations and management took corrective action and closed the recommendation related to establishing standard baseline configurations for desktops and servers.[10] However, management indicated that corrective action for the recommendations related to documenting approved deviations and monitoring for compliance with approved baselines were not completed and therefore management did not close the recommendations.

NIST SP 800-53, Revision 4, requires agencies to document and implement configuration settings for their information technology, document and approve any deviations from the configuration settings and monitor for compliance with the approved configuration settings.

If systems are not configured to minimally acceptable system configurations, there is an increased risk of vulnerabilities. In addition, without monitoring for compliance with standard baseline configurations, configurations may be intentionally or inadvertently altered from the approved baseline without management's knowledge.

[10] FY16-FISMA-NFR 1, Recommendations 2, 3, 4, and 5, *Fiscal Year 2016 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 17-03, December 22, 2016).

System Change Controls:
CNCS did not ensure proper testing of system changes. Specifically, from a sample of 21 GSS changes from the total population of 215 since October 1, 2016, we noted the following exceptions:

- 17 did not have evidence of functional test results indicating whether the system operated as intended after the change was implemented; and
- 12 did not have a completed Security Impact Analysis (SIA).[11]

Although management indicated the changes were tested, adequate documentation that testing occurred was not maintained and provided. In addition, management specified that SIAs were not required for the sampled changes tested. However, the CNCS *Cybersecurity: Security Impact Analysis SOP* list of changes requiring a SIA included all change types.

NIST SP 800-53, Revision 4, requires agencies to test system changes and analyze the changes to determine potential security impacts, prior to implementing the changes into the operational environment.

In addition, Section 4.2 of the *CNCS Office of Information Technology Configuration Management Plan*, dated March 7, 2017, specifies configuration change control includes ensuring that changes are tested. Section 4.2.2 stipulates the goal of the change assessment process is to manage and perform initial assessment of changes by performing security impact assessments. In addition, the *CNCS Cybersecurity: Security Impact Analysis Standard Operating Procedure* (SOP), Section 4, states the ISSO or Information System Stakeholder is responsible for completing the SIA.

Without following proper change management procedures, including assessment of risk and testing of system changes, security deficiencies and vulnerabilities may exist and go undetected. In addition, the system change may not operate as intended, causing functionality issues for end users.

To assist CNCS in strengthening the configuration management program, we recommend the Corporation:

> ***Recommendation 8:*** *Ensure that standard baseline configurations for all platforms in the CNCS information technology environment are appropriately implemented, tested, and monitored for compliance with established CNCS security standards. This includes documenting approved deviations from the configuration baselines with business justifications. (Modified Repeat)*
>
> ***Recommendation 9:*** *Implement improved change control procedures to ensure consistent testing and evaluation of risk for CNCS systems. The procedures should clearly define the types of changes requiring a security impact analysis and maintaining adequate documentation that a security impact analysis and functional testing occurred. (New)*

[11] According to NIST a security impact analysis is the analysis conducted by an organizational official to determine the extent to which changes to the information system have affected the security state of the system.

3. CNCS Needs to Strengthen Account Management Controls

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identity and Access Management*

Account management controls limit inappropriate access to information systems, protecting the agency's data from unauthorized modification, loss, and disclosure. For account management controls to be effective, they must be consistently implemented and monitored.

The account access review process was not effective at identifying inactive accounts or accounts belonging to separated employees or contractors. In addition, user access reviews or recertification of user accounts was not consistently performed for all systems. Specifically, we noted account management issues in the following areas:

- Access Approval
- Account Recertification
- Separated Users
- Inactive Accounts

Access Approval:

- For one of five sampled GSS privileged users (total population of 25), access was granted for privileged access to the GSS without a signed Privileged Rules of Behavior as required by CNCS policy. The CISO did not enforce CNCS policy to ensure the individual completed a Privileged Rules of Behavior prior to granting access.

Account Recertification:

- A quarterly recertification of all eSPAN and My AmeriCorps Portal user accounts was not performed for the first and second quarters of fiscal year 2017 as required by CNCS policy. The individual responsible for the recertification of the eSPAN and My AmeriCorps Portal accounts was no longer with the Corporation and management did not reassign responsibility for the quarterly account recertification.

Separated Users:

- Seven individuals retained access to the My AmeriCorps Portal application after they were separated, ranging from one to two months, from the Corporation.

  The Account Manager did not ensure the user accounts for employees who were no longer with CNCS were disabled, and the ISO and CISO did not sufficiently monitor the process to ensure CNCS policy was followed. In addition, management had not properly implemented the process for reviewing the bi-weekly report of separated employees provided by the Office of Human Capital, and ensuring accounts for those employees were disabled.

Inactive Accounts:

- Five GSS user accounts from the total population of 817 were not disabled after 30 days of inactivity in accordance with CNCS policy. As of July 14, 2017, the accounts had not been logged into for a period of 50 days to two years.

Management specified that the user whose account was not disabled for two years was in an incorrect Active Directory Organization Unit (OU) which prohibited the account from being disabled. The remaining four accounts were not captured and disabled by the automated script.

- Twenty-two My AmeriCorps Portal user accounts from the total population of 443 were not disabled after 30 days of inactivity in accordance with CNCS policy. As of July 14, 2017, 19 accounts had never logged on and three accounts had not logged on for a period of 30 to 70 days.

  Management indicated that since network accounts are automatically disabled after 30 days of inactivity, the risk for accessing My AmeriCorps Portal accounts is minimized. However, we noted issues with the automated control for disabling inactive network accounts. Furthermore, there is a possibility that active dormant accounts can be mishandled and misused, increasing the risk of unauthorized or improper access.

  A recommendation regarding disabling inactive accounts was made in the FY 2015 FISMA evaluation.[12] Management indicated that corrective action had been taken and closed the recommendation.

The CNCS Control Families document states the Information System Security Manager (ISSM), or an individual designated by the Information Security Officer (ISO), are responsible for reviewing accounts for compliance with account management requirements at least quarterly. In addition, the ISO is responsible for ensuring information system access is disabled within one working day following termination action. Finally, the ISSM, or an individual designated by the ISO are responsible for ensuring the information system automatically disables inactive accounts after 30 days.

NIST Special Publication 800-53, Revision 4, requires the following account management controls:

- Approving requests for creating information system accounts.
- Defining the frequency and implementing a process for reviewing accounts for compliance with account management requirements.
- Implementing procedures for disabling and removing system accounts.
- Defining a time period and implementing a process for automatically disabling inactive accounts.
- Obtaining a signed acknowledgment of the rules of behavior from system users prior to authorizing system access.

Without effective access controls, CNCS information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure. In addition, without performing periodic account reviews, system users whose job duties may have changed could retain access no longer required. Lastly, inactive accounts that are not disabled in accordance with agency policy, and user accounts that are not disabled when employees separate, may be misused or susceptible to a ‘brute force’ attack to gain access to the Corporation’s data and sensitive information.

[12] FY15-FISMA-NFR 2, Recommendations 1, *Fiscal Year 2015 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 16-03, November 13, 2015).

To assist CNCS in strengthening the account management controls, we recommend the Corporation:

> ***Recommendation 10****: Implement improved processes to ensure that all privilege users sign the Privileged Rules of Behavior prior to being granted privileged access to the network. The process should include a periodic audit of the account provisioning process of each privileged user by the CISO to ensure all requirements for granting privileged access are met. (New)*
>
> ***Recommendation 11****: Implement improved processes to ensure quarterly recertification of eSPAN and My AmeriCorps Portal accounts are completed in accordance with the CNCS access control policy and related standard operating procedures. (New)*
>
> ***Recommendation 12****: Implement improved processes to ensure system accounts are disabled upon termination of an individual's employment in accordance with CNCS policy. The process should include:*
>
> - *A review of the bi-weekly listing of employees who are no longer with CNCS from the Office of Human Capital by the Account Manager, ISO and the CISO.*
> - *Procedures for the ISO to verify on a weekly basis that the Account Manager disabled the accounts.*
> - *Procedures for the CISO to audit the account management process on a monthly basis to ensure accounts for separated employees are disabled. (New)*
>
> ***Recommendation 13****: Implement improved processes to ensure inactive accounts are disabled in accordance with CNCS policy. The process should include:*
>
> - *Monitoring the automated script for disabling accounts after 30 days of inactivity on an ongoing basis to ensure it is operating as intended.*
> - *Procedures for the CISO to audit inactive account listings on a monthly basis to ensure the process for disabling inactive accounts is followed. (Modified repeat)*

4. CNCS Must Implement Multifactor Authentication for Privileged and Non-Privileged Accounts

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identity and Access Management*

Multifactor authentication requires two or more credentials when logging on to information systems. Credentials include something you know, such as a password, something you have like a Personal Identification Verification (PIV) card or something you are, such as a fingerprint.

CNCS did not implement PIV multifactor authentication for local and network access for privileged users and for network access for non-privileged users. Currently, non-PIV multifactor authentication of authorized users not using CNCS furnished computers was only implemented for remote access to the network.

The CISO stated that CNCS once again did not receive funding during FY 2017 for implementing PIV multifactor authentication. A subsequent request for funding was made again for FY 2018 for the required resources. In addition, CNCS has created a project plan and an active working group that is making progress towards identifying technical requirements necessary for implementation of PIV multifactor authentication for network access.

NIST requires information systems to uniquely identify and authenticate users prior to granting access. Multifactor authentication requires users to authenticate with additional credentials other than solely a user name and password. Examples of additional credentials are a token or PIV credentials issued by federal agencies.

In addition, NIST SP 800-53, Revision 4, requires information systems categorized as moderate to implement multifactor authentication: 1) for network access to privileged accounts, 2) for network access to non-privileged accounts, and 3) for local access to privileged accounts.

OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, requires federal agencies to have 100 percent of privileged users and 85 percent of non-privileged users authenticate through PIV credentials.

Without PIV multifactor authentication for local and network access for privileged user accounts, there is an increased risk of unauthorized access at a privileged level by an unauthorized user. Unauthorized privileged access can allow an individual to inappropriately create, delete and modify users and services running on the network as well as gain access to all data stored on the network and its systems to include GSS, eSPAN, and Momentum. In addition, without PIV multifactor authentication for network access for non-privileged user accounts, there is increased risk of unauthorized access to CNCS information, including PII, and information systems by an unauthorized user decreasing the confidentiality and integrity of data.

To assist CNCS in strengthening identification and authentication controls, we recommend the Corporation:

> ***Recommendation 14****: Implement PIV multifactor authentication for local and network access for privileged users. (New)*
>
> ***Recommendation 15****: Implement PIV multifactor authentication for network access for non-privileged users. (New)*

5. CNCS Needs to Enhance the Review and Analysis of Momentum Audit Logs

Cybersecurity Framework Domain: *Detect*
FY 17 FISMA IG Metric Area: *Information Security Continuous Monitoring*

CNCS did not capture the Momentum Oracle security logs into its Splunk[13] tool, an event[14] correlation tool used for audit log review, analysis and reporting. The event and trend analysis to investigate security events is required by NIST for information systems categorized as moderate.[15]

CNCS began the implementation of the Splunk tool in November 2015 to replace an older network monitoring and audit log analysis software. In FY 2017, CNCS began the process of aggregating the Momentum Oracle logs into Splunk; however, the collection of the logs was not completed due to connectivity issues that occurred between Oracle and the Splunk tool during testing. Management indicated that they are working to resolve these issues.

NIST requires information systems to audit events deemed significant to the security of the information system and the environment in which those systems operate. In addition, the audit events must be reviewed, analyzed and reported in order to respond to and timely remediate incidents. In addition, NIST SP 800-53, Revision 4, requires organizations to analyze and correlate audit records across different repositories to gain organization-wide situational awareness.

If all critical systems and platforms are not incorporated into the audit log collection process, CNCS cannot maintain an understanding of the security events occurring from an organizational risk perspective. This diminishes the Corporation's ability to detect and address these threat patterns in order to improve the Corporation's information security state.

To assist CNCS in strengthening the audit review, analysis and reporting process, we recommend the Corporation:

> ***Recommendation 16**: Complete the process for aggregating the Momentum Oracle database security logs into the Splunk tool. (New)*
>
> ***Recommendation 17:** Implement policies and procedures for the review, analysis, and reporting of the Momentum Oracle security logs. The procedures should clearly define activity to be reviewed, review frequency, assignment of responsibility and the preparation, storage and retention of artifacts to demonstrate reviews were performed. (New)*

[13] Splunk collects and indexes log data, correlates events by discovering relationships between seemingly unrelated events in the log data, and automatically generates alerts for critical events. In addition, dashboards can be created for monitoring events and updating the incident response team and management.

[14] A security event is a change from what is expected in how an information system functions, signifying that a security policy may have been breached or security measures may have failed.

[15] Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, provides guidance for determining the security category of federal information systems based on confidentiality, integrity and availability.

6. CNCS Needs to Enhance the Personnel Screening Process

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identity and Access Management*

The purpose of performing background checks is to ascertain the suitability of an individual for a specific position. Screening should be appropriate to the risk and significance of the harm an individual could cause to the Corporation. Therefore, when screening individuals, a risk designation based on sensitivity level of the position must be considered.

CNCS did not ensure employees with privileged access to the critical Momentum system underwent appropriate background investigations. Specifically, three out of the five privileged Momentum users had background investigations below the level commensurate with the risk associated with their assigned positions. These individuals had a National Agency Check with Inquiries (NACI) investigation. The privileged users were CNCS employees with sensitive roles and permissions in the Momentum application that would require a higher level of background investigation.

Management indicated that it recognized the weakness of these background investigations and that the Office of Human Capital is updating a role designation chart specifying the type of investigation required by position and sensitivity levels.

According to NIST SP 800-53, Revision 4, organizations are to screen individuals prior to authorizing access to the information system. Organizations can define different rescreening conditions and frequencies for personnel accessing information systems based on types of information processed, stored, or transmitted by the systems.

Without sufficient screening of employees and contractors, CNCS cannot validate that individuals are suitable for the level of system access or job responsibilities assigned to them.

To assist CNCS in strengthening the personnel screening process, we recommend the Corporation:

> ***Recommendation 18:*** *Complete the updates to the role designation chart specifying the type of background investigation required by position and sensitivity levels. (New)*
>
> ***Recommendation 19:*** *Document and implement a process to ensure background investigations for CNCS employees and contractors are performed at a level commensurate with the risk associated with their assigned positions. (New)*

7. CNCS Needs to Strengthen Contingency Planning Controls

Cybersecurity Framework Domain: *Recover*
FY 17 FISMA IG Metric Area: *Contingency Planning*

It is critical that organizations have a process in place to minimize the risk of unintended interruptions, and recover critical operations when interruptions transpire. This includes a process for consistently backing up agency data, documenting a contingency plan, and testing the contingency plan at a specified frequency to determine the effectiveness of the plan. The results of the testing exercise should be analyzed, and the agency should update the contingency plan to increase its usefulness, along with other facility level plans.

We noted the following issues related to contingency planning controls:

- CNCS did not complete an after-action report that specified whether Recovery Time Objectives (RTOs) were met, and any lessons learned for the GSS/eSPAN disaster recovery test conducted in June 2017. A disaster recovery test checklist was documented that recorded whether each checklist step was completed.

  Discussions with the CISO revealed that CNCS relied on the disaster recovery test results that noted successful completion of the test steps, rather than completing an after action report and lessons learned. Without analyzing information collected during the disaster recovery test, there is a risk that the disaster recovery plan will not be updated to improve the effectiveness of the plan.

- The CNCS Continuity of Operations Plan (COOP) was not up-to-date. Specifically it did not reflect the Business Impact Analysis (BIA) or updates to the Disaster Recovery Plan (DRP) that were completed since last year.

  The FY 2014 FISMA evaluation[16] noted recommendations for the Corporation to develop individual BIAs for each critical system, to update the DRP to cover the entire Corporation and all critical IT contractors, and to update the COOP based on revisions to the BIA and DRP. Based on our assessment, we noted that the BIA was completed and the DRP was updated; however, the COOP was not updated to reflect the changes to the BIA and DRP.

  Management indicated that the corrective action to update the COOP had not been completed, the recommendation was not closed, and the scheduled completion date was December 29, 2017. Without an up-to-date COOP, CNCS cannot guarantee the continuity of operation of all the Corporation's mission-essential functions in the occurrence of threat events.

[16] FY14-FISMA-NFR 14, Recommendation 1, Part E, *FY14 Federal Information Security Management Act (FISMA) Independent Evaluation for FY 2014* (OIG Report No. 15-03, November 14, 2014).

- CNCS did not document and implement a Service Level Agreement (SLA) or performance metrics to ensure that GSS backups are performed in accordance with contractual requirements. The FY 2016 FISMA evaluation[17] noted a recommendation related to this control weakness. However, management indicated that corrective action related to the SLA had not been taken, the recommendation remains open, and the scheduled completion was October 31, 2017. Without ensuring successful data backup, CNCS is at risk of data loss, impacting the ability of the Corporation to perform its mission.

NIST SP 800-34, *Contingency Planning Guide for Federal Information Systems*, specifies that results of the test are documented in an After Action Report, and Lessons Learned are developed for updating information in the Information System Contingency Plan.

In addition, NIST SP 800-34, states, "contingency plans must be written in coordination with other existing plans associated with systems. Such plans include facility level plans such as the COOP."

Furthermore, NIST SP 800-53, Revision 4, requires that organizations perform backups of information contained in its information systems at a defined frequency.

To assist CNCS in strengthening the contingency planning process, we recommend the Corporation:

> ***Recommendation 20:*** *Complete a formal after action report for the GSS/eSPAN disaster recovery test and ensure lessons learned are reviewed and corrective actions are taken. (New)*
>
> ***Recommendation 21:*** *Update the COOP based on revisions to the BIA and DRP. (Repeat)*
>
> ***Recommendation 22:*** *Develop and implement a SLA or performance metrics to ensure that GSS backups are performed in accordance with contractual requirements. (Repeat)*

[17] FY16-FISMA-NFR 2, Recommendation 3, *Fiscal Year 2016 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 17-03, December 22, 2016).

Facility Level Findings

8. CNCS Needs to Consistently Enforce an Agency-wide Information Security Program Across the Enterprise

Cybersecurity Framework Domain: *Detect*
FY 17 FISMA IG Metric Area: *Risk Management*

Effective system security begins with strong governance, including agency level oversight and controls monitoring of CNCS NCCC campuses and State Offices. The combination of agency-level and facility level control weaknesses can increase the risk of unauthorized access to the Corporation's systems, affecting the reliability and security of the data and information.

During site visits to the CNCS Vicksburg and Denver NCCC campuses and State Offices, we noted control weaknesses related to the following areas:

- Vulnerability and patch management;
- Access controls for mobile devices;
- Protection of personally identifiable information (PII);
- Audit logging;
- Inventory management; and
- Physical and environmental protection.

Many of these weaknesses identified can be attributed to an inconsistent enforcement of the agency-wide information security program across the enterprise and ineffective communication between CNCS management and the individual field offices. Therefore, CNCS needs to improve its performance monitoring to ensure controls are operating as intended at all facilities and communicate security deficiencies to the appropriate personnel to take responsibility for implementing corrective actions and ensuring those actions are taken.

To assist CNCS in strengthening its agency-wide information security program, we recommend the Corporation:

> ***Recommendation 23:*** *Enforce the agency-wide information security program across the enterprise and improve effective communications between CNCS management and the individual field offices. CNCS should improve its performance monitoring to ensure controls are operating as intended at all facilities and communicate security deficiencies to the appropriate personnel to take responsibility for implementing corrective actions and ensuring those actions are taken. (New)*

The following are the details regarding these findings.

9. CNCS Must Improve Its Vulnerability and Patch Management Controls

Cybersecurity Framework Domain: *Detect*
FY 17 FISMA IG Metric Area: *Risk Management*

Patch management is the process for identifying, acquiring, installing, and verifying patches for products and systems, and is an important component of vulnerability management. Patches correct security vulnerabilities and functionality problems in software. Applying patches to eliminate these vulnerabilities significantly reduces the risk of exploitation. Also, patches are usually the most effective way to mitigate software flaw vulnerabilities, and are often the foundation for an effective vulnerability management program.

Unpatched and unsupported software exposed the Denver NCCC campus and Denver State Office network to critical and high severity vulnerabilities. Specifically, we noted the following:

- Based on independent scans of 22 computing devices, using the Nessus software tool, 23 critical and 324 high risk vulnerabilities related to patch management, configuration management, and unsupported software were identified at the Denver NCCC campus. Additionally, from a scan of 7 computing devices at the Denver State Office, one critical and six high risk vulnerabilities related to patch management, configuration management, and unsupported software were identified. Many of the patch management vulnerabilities were publicly known before 2016, such as those related to Adobe Acrobat, Oracle, and Cisco WebEx. According to industry research, six of the top ten vulnerabilities in 2016 were with Adobe software, all of which are linked to criminal and state-sponsored actors.

- Microsoft Internet Explorer was missing required registry changes at both the Denver NCCC campus and Denver State Office.

- The unsupported software was related to the following:
  - Adobe Acrobat (no longer supported as of November 15, 2015) was identified at the Denver NCCC campus
  - Adobe Photoshop (no longer supported as of February 28, 2015) was identified at the Denver NCCC campus
  - Microsoft XML Parser and XML Core Services (no longer supported as of April 12, 2014) was identified at the Denver NCCC campus and Denver State Office

A recommendation to strengthen the vulnerability scanning process was made in the FY 2014 FISMA evaluation[18] and an additional five recommendations were made in the FY 2016 FISMA evaluation.[19] Management indicated that corrective action had not been completed for the 2014 recommendation, and that corrective action had been taken for 4 of the 5 FY 2016 recommendations, and had closed them. The other FY 2016 recommendation was still open.

[18] FY14-FISMA-NFR 2, Recommendation 8, *FY14 Federal Information Security Management Act (FISMA) Independent Evaluation for FY 2014* (OIG Report No. 15-03, November 14, 2014).
[19] FY16-FISMA-NFR 1, Recommendations 1, 2, 3, 4, and 5, *Fiscal Year 2016 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 17-03, December 22, 2016).

NIST SP 800-53, Revision 4, requires organizations to scan their information systems for vulnerabilities, analyze the scan reports and remediate vulnerabilities within a specified timeframe. Vulnerability scanning includes scanning for unpatched, outdated operating systems and applications, and configuration settings.

In addition, the CNCS Control Families document states the ISSO is responsible for:

- Scanning for vulnerabilities in the information system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported
- Analyzing vulnerability scan reports and results from security control assessments
- Remediating legitimate vulnerabilities in accordance with an organizational assessment of risk
    - Critical - within 48 hours of CISO approval after testing
    - High - within 30 days
    - Moderate - within 90 days
    - Low - within 180 days
- Sharing information obtained from the vulnerability scanning process and security control assessments with Cybersecurity to help eliminate similar vulnerabilities in other information systems (i.e., systemic weaknesses or deficiencies)

The overall deployment of vendor software patches and system upgrades by the GSS support team under the direction of the CNCS OIT to mitigate the vulnerabilities was decentralized, inconsistent, and not effective across all facilities. In addition, the GSS ISSO did not have a process in place to ensure the timely correction of identified information system flaws and did not install security-relevant software and firmware updates within the defined guidelines.

The Denver NCCC campus and State Office may likely be at risk due to unpatched systems. Vulnerabilities could be exploited to take control of systems, to cause a denial of service attack, or to allow unauthorized access to Denver NCCC campus and State Office applications. In addition, software that is missing security patches or software for which the vendor no longer provides updated security patches could leave security weaknesses unfixed, exposing those systems to increased attack methods compromising the confidentiality, integrity, and availability of data.

To assist CNCS in strengthening its vulnerability management program, we recommend the Corporation:

> ***Recommendation 24:*** *Ensure the CNCS Office of Information Technology monitor and promptly install patches and antivirus updates when they are available from the vendor across the enterprise. Enhancements should include:*
>
> - *Improve the effectiveness of patching network devices and servers.*
> - *Ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer.*
> - *Ensure vulnerability remediation for network devices and servers is addressed or the exposure to unpatchable vulnerabilities is minimized.*
> - *Monitor and enforce Team Lead laptops' compliance with security updates and update of antivirus signatures. (Modified Repeat)*

10. CNCS Needs to Strengthen Access Controls for Mobile Devices

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identity and Access Management*

A mobile device is a hand-held computer such as a smartphone, tablet, or laptop. Mobile devices also require adequate protection to protect the confidentiality and integrity of CNCS data. According to NIST, applying protective controls for mobile devices includes, for example, "configuration management, device identification and authentication, implementation of mandatory protective software (e.g., malicious code detection, firewall), scanning devices for malicious code, updating virus protection software, scanning for critical software updates and patches, conducting primary operating system (and possibly other resident software) integrity checks, and disabling unnecessary hardware (e.g., wireless, infrared)."

Mobile devices provided to the Vicksburg and Denver NCCC campus personnel such as Team Lead laptops and Verizon contract phones were not securely configured and managed. Both devices were used by Team Leads as the primary means of communication and conducting CNCS NCCC campus business. Specifically, we noted:

- NCCC campus Team Lead laptops were purchased by CNCS Headquarters, configured with encryption software and an encryption password and shipped to the NCCC campus by CNCS OIT. The Vicksburg NCCC campus taped the hard disk encryption password to the Team Lead laptop in clear sight of office personnel. The privileged password is the same as configured for every Team Lead laptop, and is reused year after year.

- The Team Lead laptops at both NCCC campuses were not configured to require a password for the general user. In addition, the laptops were not monitored for compliance with security updates and antivirus signatures.

- Both NCCC campuses did not re-image IT assets before re-issuing the assets to a new user. The current process at the Vicksburg NCCC was to create a new user account before re-issuing the assets, whereas the Denver NCCC would only delete the previous user's files before re-issuing.

- The Vicksburg and Denver NCCC campus Team Lead are issued non-governmental Google mail (Gmail) accounts that were used for government business to include communication with project sponsors. In addition, the Gmail accounts were shared, class after class, and the password was not changed.

- The cellphones procured by the Vicksburg NCCC campus for the Team Leads were not configured to require enabling of security features, including the use of a pin to unlock the phone.

These issues occurred because the GSS ISSO had not established usage restrictions, configuration and connection requirements, nor implementation guidance for mobile devices that do not connect to the CNCS general support system, such as the Team Lead laptops and cell phones. In addition, the GSS ISSO did not enforce the automatic updates of malicious code protection mechanisms to all information systems. Furthermore, the NCCC campuses did not have a dedicated IT resource to implement and monitor IT security policies and procedures for Team Lead laptops, mobile devices, nor the Labs.

The CNCS Control Families document states the ISO is responsible for:

- Establishing usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices.
- Centrally managing malicious code protection mechanisms.
- Ensuring the information system automatically updates malicious code protection mechanisms.

The likelihood of unauthorized access and unavailability of data was high as passwords were not restricted from public view and not periodically changed to ensure inappropriate or unauthorized access to program information. In addition, the lack of security features and current antivirus signatures increases the risk that vulnerabilities could be exploited leaving the NCCC campuses susceptible to malicious software and loss of confidentiality, integrity, and availability of data.

To assist CNCS in strengthening access controls for mobile devices, we recommend the Corporation:

> ***Recommendation 25:*** *Ensure the CNCS GSS Information System Owner establishes and enforces the policy for mobile devices that do not connect to the CNCS GSS to include usage restrictions, configuration and connection requirements, and implementation guidance. (New)*

Recommendation 26: *Ensure the facilities implement the following in regards to protection of mobile devices:*

- *Enforce the prohibition of displaying passwords in public view*
- *Require the use of passwords on mobile computer assets for all users*
- *Change passwords and re-image IT assets upon the separation of the previous user*
- *Monitor Team Lead laptops for compliance with security updates and antivirus signatures*
- *Prohibit the use of non-governmental CNCS issued email accounts*
- *Configure cell phones to require the enabling of security functions (New)*

Recommendation 27: *Ensure the facilities implement the following in regards to protection of mobile devices:*

- *Require the use of passwords on mobile computer assets for all users*
- *Change passwords and re-image IT assets upon the separation of the previous user*
- *Prohibit the use of non-governmental CNCS issued email accounts (New)*

11. CNCS Needs to Strengthen Monitoring of Wireless Access Connections

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identity and Access Management*

Wireless access connections can be vulnerable access points for unauthorized individuals to access CNCS data. The Vicksburg NCCC wireless network is an open network which requires no password for a user to connect to the access point and use the internet. Any user in range of the Vicksburg NCCC can connect to the wireless network and freely use the internet. A malicious user could connect to the wireless network and launch an attack against all connected devices or use the internet connection for malicious activities with no way for the Vicksburg NCCC to know these activities were happening. For that reason, wireless access connections should be logged and monitored to ensure only authorized individuals are accessing the network.

The Vicksburg NCCC has implemented two instances of continuous monitoring for its public wireless network and campus Computer Lab computers. These two methods use a product called Cisco Umbrella formerly known as OpenDNS. While the system was functional, the events detected were not being acted upon, as no one was monitoring the logs.

There were two separate accounts for the OpenDNS service, one for the wireless environment that is owned and operated by the Federal Emergency Management Agency (FEMA) and the other for the computer lab environment. The Vicksburg NCCC campus personnel are able to use the wireless network if the campus' network interconnection to the CNCS enterprise wide area network is slow. The facility was not receiving reports for the wireless environment due to the separation of the individual assigned the user name and password for that account. Management did not ensure the account for administering and reviewing the OpenDNS reports for the wireless network were assigned to another individual.

NIST SP 800-53, Revision 4, states that audit records are required to "contain information that established what type of event occurred, when the event occurred, where the event occurred, the source of the event, the outcome of the event, and the identity of any individuals for subjects associated with the event."

NIST also states that agencies are required to define the frequency of, and review and analyze information system audit records for signs of inappropriate or unusual activity and report issues to appropriate personnel. Audit review, analysis and reporting includes monitoring of wireless connectivity.

Lack of access monitoring can result in unauthorized use of or compromise of information resources and NCCC campus data without Vicksburg NCCC campus's awareness. Further, without the ability to supervise and restrict inappropriate websites, the Vicksburg NCCC campus was at risk of inappropriate use of resources exposing their systems to computer viruses and malicious software and increasing the possibility of unauthorized access to sensitive data.

To assist CNCS in strengthening monitoring of wireless access connections, we recommend the Corporation:

> ***Recommendation 28:*** *Ensure the Vicksburg NCCC campus implements the following regarding the OpenDNS service:*
>
> - *Remove the unnecessary account to the OpenDNS service, and create a new account for administrative access.*
> - *Review the OpenDNS reports for the wireless network. (New)*
>
> ***Recommendation 29:*** *Configure CNCS issued laptops to deny the use of the FEMA wireless network by service set identifier (SSID). (New)*

12. CNCS Needs to Strengthen the Protection of Personally Identifiable Information

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identify and Access Management*

We noted that PII was stored in a Vicksburg NCCC campus room, locked by hard keys, in the basement of Green Hall. In addition, the storage room had a window to the exterior and the door had a glass window pane. Further, the storage room did not have a badge reader or camera to record entry to and exit from the room.

The Vicksburg NCCC campus management did not ensure adequate protective controls were in place to protect PII in the storage room to validate who was accessing the room. As a result, management was not able to determine who accessed the storage room due the lack of a badge reader or a camera to record who was accessing the storage room. Consequently, the Vicksburg NCCC campus may be exposed to inappropriate or unauthorized access to PII which may result in the loss of confidentiality of the information stored leading to personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

NIST SP 800-122, *Guide to Protecting the Confidentiality of Personally Identifiable Information (PII),* defines PII as "any information about an individual maintained by an agency, including (1) any information that can be used to distinguish or trace an individual's identity, such as name, social security number, date and place of birth, mother's maiden name, or biometric records; and (2) any other information that is linked or linkable to an individual, such as medical, educational, financial, and employment information."

NIST SP 800-53, Revision 4, requires organizations to "physically control and securely store media within controlled areas." "Information system media includes both digital and non-digital media. Digital media includes, for example, diskettes, magnetic tapes, external/removable hard disk drives, flash drives, compact disks, and digital video disks. Non-digital media includes, for example, paper and microfilm."

To assist CNCS in strengthening controls regarding the protection of PII, we recommend the Corporation:

> ***Recommendation 30:*** *Ensure the Vicksburg NCCC campus implements additional monitoring controls to have an automated record of who is accessing the files in the storage room. (New)*

13. CNCS Needs to Improve the Information Technology Asset Inventory Management Process

Cybersecurity Framework Domain: *Identify*
FY 17 FISMA IG Metric Area: *Risk Management*

Applying adequate security controls to CNCS information technology assets requires knowing what those assets are and where they are located. NIST SP 800-53, Revision 4, requires organizations to develop and document an accurate information system component inventory.

We noted the following issues related to the completeness and accuracy of the IT physical asset inventory:

- The OIT Headquarters and Denver NCCC campus asset inventory was inaccurate. For example:
    - A switch that was observed on-site was not listed on either the Headquarters' system inventory or the Denver FasseTrack Freedom's inventory. Upon notification of the issue, management added the switch to the OIT Headquarters inventory.
- The OIT Headquarters inventory for the Vicksburg NCCC campus was inaccurate. For example:
    - 5 out of a sample of 15 assets had their inventory status listed incorrectly in the OIT Headquarters inventory. Specifically:
        - 3 were listed as in use, but were in storage at the Vicksburg NCCC campus.
        - 2 were listed as in use, but were returned to OIT Headquarters.

The FY 2015 FISMA evaluation noted a recommendation to perform biannual physical IT inventory audits at Headquarters and field offices to ensure the IT inventory list and assignments of physical IT assets are accurate.[20] Management indicated that corrective action had been taken and closed the recommendation. However based on our evaluation, we noted that CNCS partially remediated the FY 2015 FISMA recommendation.

The Headquarters and NCCC campus inventories were maintained independently by the respective parties and the FasseTrack system was not integrated with the Headquarters inventory. As a result, a manual reconciliation is required to update the respective inventories.

Incomplete or inaccurate inventories could result in a loss of confidentiality and waste. Stolen or misplaced computing equipment could put CNCS at a risk of loss of control of their data and potentially PII. This may also cause a strain on the CNCS budget as unplanned and unnecessary spending may be required to replace stolen or misplaced computing equipment.

To assist CNCS in strengthening controls regarding inventory management, we recommend the Corporation:

> ***Recommendation 31:*** *Document and implement improved procedures over the manual reconciliations performed to ensure the accuracy and completeness of the Headquarters inventory and the FasseTrack system. (Modified Repeat)*

14. CNCS Needs to Improve Physical and Environmental Protection Controls

Cybersecurity Framework Domain: *Protect*
FY 17 FISMA IG Metric Area: *Identity and Access Management*

Physical controls should be in place to protect CNCS facilities from unauthorized access. This includes controls for granting access only to authorized individuals, and monitoring who accesses CNCS facilities via badge readers, cameras and security guards. Environmental controls can help prevent or alleviate potential damage to CNCS facilities and interruptions to the availability of information systems. Examples of environmental controls include:

- Fire extinguishers and fire-suppression systems
- Smoke detectors
- Water detectors
- Backup power supplies

[20] FY15-FISMA-NFR 4, Recommendation 3, *Fiscal Year 2015 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 16-03, November 13, 2015).

The following issues were noted regarding physical and environmental protection at the NCCC campuses and State Offices:

- The Vicksburg NCCC campus main camera that is situated to record the front entry did not save recorded footage to a hard drive for review at a later time for approximately six months. In addition, there were no NCCC campus personnel actively monitoring the camera system that recorded entry points to the main building. Furthermore, review of the recordable data was only performed as needed.

  A lightning strike caused the main campus camera to become inoperable and due to the existence of other cameras and a guard at the front door, management did not prioritize replacing the damaged video storage device right away. In addition, the Vicksburg NCCC campus did not have the resources to monitor camera recordings.

  As a result, the Vicksburg NCCC campus would not have video recordings to review in an event an investigation is needed. In addition, there may be a delayed response to an incident, since management does not review video records in real time.

- An Uninterruptable Power Supply (UPS) at the Denver and Jackson State Offices displayed an error to warn the State Offices that the battery needed to be changed; however, neither State Office monitored the function of the UPS or reported the error message for resolution. The battery was both a fire hazard and a concern for the continuation of operations in the event of a power outage.

  Without emergency power, the Denver and Jackson State Offices may not be able to conduct a controlled shut down of their computers in the event of a power outage, which could result in a loss of data.

- The Jackson State Office did not have a fire extinguisher or smoke detectors due to management oversight. Without fire extinguishers or smoke detectors, the Jackson State Office would not be able to extinguish or be immediately alerted of smoke or fire, and records in hard copy may be destroyed.

NIST SP 800-53, Revision 4, requires organizations to implement the following physical access controls:

- Maintain and review physical access audit logs for entry and exit points defined by the agency.
- Control access to publicly assessable areas within the facility with security safeguards, such as cameras and monitoring by guards.

In addition, NIST SP 800-53, Revision 4, stipulates the organization should provide a short-term uninterruptible power supply to provide emergency power in the event the main power source is lost. In addition, organizations should maintain fire suppression and detection systems for their information systems.

To assist CNCS in strengthening physical and environmental protection controls, we recommend the Corporation:

> ***Recommendation 32:*** *Ensure the Vicksburg NCCC campus implements corrective actions to ensure video recordings of the main entry are captured and a process is implemented to monitor the camera feeds. (New)*
>
> ***Recommendation 33:*** *Ensure the Denver and Jackson State Offices implement corrective actions to monitor the function of the UPS and resolve the UPS error messages. (New)*
>
> ***Recommendation 34:*** *Ensure the Jackson State Office installs a fire extinguisher and smoke detectors. (New)*

SCOPE AND METHODOLOGY

Scope

We conducted this evaluation in accordance with the *Quality Standards for Inspection and Evaluation*, issued by the Council of Inspectors General on Integrity and Efficiency. The evaluation was designed to assess the effectiveness of CNCS's information security program in accordance with FISMA, OMB requirements, and NIST guidance.

The overall scope of the FISMA evaluation was the review of relevant security programs and practices to report on the effectiveness of the CNCS's agency-wide information security program in accordance with the OMB's annual FISMA reporting instructions. We reviewed controls specific to FISMA reporting, including the process and practices CNCS implemented for safeguarding PII and reporting incidents involving PII, protecting sensitive corporate information, and management oversight of contractor-managed systems.

The evaluation included the testing of select management, technical, and operational controls outlined in NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, for the following information systems:

- GSS
- eSPAN
- My AmeriCorps Portal (a subsystem of eSPAN)
- Momentum

Our evaluation included an assessment of information security controls both at the enterprise and at the facility level (NCCC and State Offices). The enterprise level assessment was conducted at the CNCS Headquarters in Washington, D.C., from May 18, 2017 to September 30, 2017. The facility level assessment included on-site security assessments at the Vicksburg, Mississippi and Denver, Colorado NCCCs and State Offices including:

- Review of desktop or laptop configuration management and encryption
- Review of proper usage of CNCS network resources
- Review of physical security
- Review of rogue connections
- Review of network access by eligible CNCS personnel and members
- Review of the handling of PII
- A sampled check for inappropriate images or audio files found on laptops or desktops.

In addition, a network vulnerability assessment was conducted at the Denver NCCC and State Office.

The evaluation also included a follow up on prior year FISMA evaluation recommendations[21] to determine if CNCS made progress in implementing the recommended improvements concerning its information security program.

[21] *Fiscal Year 2016 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 17-03, December 22, 2016).

Methodology

Following the framework for minimum security controls in NIST SP 800-53, Revision 4, certain controls were selected from NIST security control families[22] associated with FY 2017 IG FISMA metric domains aligned with the Cybersecurity Framework Security Functions. We reviewed the selected controls over four systems.

To accomplish our objective we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to CNCS's information security program, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan and continuous monitoring plan.
- Tested system processes to determine the adequacy and effectiveness of selected controls.
- Reviewed the status of recommendations in the FY 2016 FISMA report, including supporting documentation to ascertain whether the actions taken addressed the weakness.[23]

In testing the effectiveness of the security controls, we exercised professional judgment in determining the number of items selected for testing and the method used to select them. We considered relative risk, and the significance or criticality of the specific items in achieving the related control objectives. In addition, we considered the severity of a deficiency related to the control activity and not the percentage of deficient items found compared to the total population available for review. In some cases, this resulted in selecting the entire population. However, in cases that we did not select the entire population, the results cannot be projected, and if projected, may be misleading.

[22] Security controls are organized into families according to their security function—for example, access controls.

[23] Ibid. footnote 21.

STATUS OF PRIOR YEAR RECOMMENDATIONS

Tables 5, 6 and 7 summarize the status of our follow up related to the standing of prior year recommendations reported for the FY 2014,[24] 2015[25] and 2016[26] FISMA evaluations.

From the FY 2014, 2015 and 2016 FISMA evaluations, the Corporation implemented corrective actions to fully close 19 prior year recommendations. In addition, the Corporation partially closed one prior year recommendation.

Table 5: Status of Prior Year FY 2014 Recommendations

FISMA NFRs	FY 2014 FISMA Evaluation	CNCS Position on Status	Auditor Evaluation of CNCS' Status
FY 14 - FISMA - NFR 1	**Recommendation 3:** Formalize ISCM processes to include the following:		
	Part D: Correlation and analysis of security-related information generated by assessments and monitoring.	Closed	Agree
	Part E: Response actions to address the results of the analysis	Closed	Agree
FY 14 - FISMA - NFR 2	**Recommendation 8:** Ensure that an appropriately configured vulnerability scan is conducted monthly against all information system components, including servers, routers, desktops, network printers, scanners, and copiers.	Open	Agree Modified Repeat, refer to Finding 8
	Recommendation 1: Develop, document, and implement a vulnerability scanning process that incorporates periodic discovery scans, review and remediation of authentication failures, and periodic reconciliations to confirm that all known servers and network devices were scanned.	Closed	Agree

[24] *FY14 Federal Information Security Management Act (FISMA) Independent Evaluation for FY 2014* (OIG Report No. 15-03, November 14, 2014).

[25] *Fiscal Year 2015 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 16-03, November 13, 2015).

[26] Ibid. footnote 19.

FISMA NFRs	FY 2014 FISMA Evaluation	CNCS Position on Status	Auditor Evaluation of CNCS' Status
	Recommendation 2: Obtain technical training on the Corporation's vulnerability scanning solution to increase awareness of vulnerability scanning best practices and recommended configurations.	Closed	Agree
	Recommendation 3: Retain professional services from the software vendor or other independent expert to conduct an independent review of the Tenable Nessus installation and obtain recommendations for enhancing the vulnerability reporting solution.	Closed	Agree
	Recommendation 4: Require that the MITS contractor periodically change the password for privileged accounts (i.e., Domain Admin, root) used to conduct weekly vulnerability scanning.	Closed	Agree
	Recommendation 5: Perform authenticated vulnerability scans weekly of the critical Corporation applications and databases (eSPAN, eGrants, MyAmeriCorps portal).	Open	Agree Modified Repeat, refer to Finding 8
FY 14 - FISMA - NFR 6	**Recommendation 3:** Consider contracting for a network penetration study and including the Corporation's voice network within the scope of the study.	Closed	Agree
	Recommendation 5: Correct factual inaccuracies in the SSP for the LAN/WAN regarding the Corporation's VoIP infrastructure and identify compensating controls to address the risks associated with commingling data and VoIP networks.	Closed	Agree
FY 14 - FISMA - NFR 9	**Recommendation 1:** Document and fully implement a comprehensive and enterprise-wide risk management process, including the following:		

FISMA NFRs	FY 2014 FISMA Evaluation	CNCS Position on Status	Auditor Evaluation of CNCS' Status
	Part A: Addressing and capturing risk at the organizational level (i.e., Tier 1), providing the context for all risk management activities carried out by the Corporation in order to understand where risk resides for prioritization of remediation strategies	Open	Agree Modified Repeat, refer to Finding 1
	Part B: Addressing and capturing risk at the mission/business process level (i.e., Tier 2), including clearly assigning ownership and responsibilities for executing risk management processes at this level.	Open	Agree Modified Repeat, refer to Finding 1
	Part C: Integrating Tier 1 and 2 Level activities and linking them to Tier 3 Level activities related to implementation, operation, and monitoring of Corporation information systems.	Open	Agree Modified Repeat, refer to Finding 1
FY 14 - FISMA - NFR 10	**Recommendation 2:** Establish security assessment standards, to ensure consistency and quality, such as:		
	Part A: Sampling plan	Closed	Agree
	Part B: Standard test cases	Closed	Agree
	Recommendation 5: Update the SSPs for eSPAN, Momentum, and LAN/WAN to ensure:		
	Part C: Responsibility for implementing each NIST SP 800-53 control is clearly delineated between the Corporation and IT vendor.	Closed	Modified Repeat, refer to Finding 1
	Part D: SSPs accurately describe the implementation details for the base NIST SP 800-53 security and privacy controls and required control enhancements.	Closed	Modified Repeat, refer to Finding 1

FISMA NFRs	FY 2014 FISMA Evaluation	CNCS Position on Status	Auditor Evaluation of CNCS' Status
	Recommendation 7: Develop and implement an assessment approach for testing common and privacy controls that includes continuous monitoring aspects, such as the monitoring of audit logs, error reports, and performance metrics.	Closed	Agree
	Recommendation 8: Annually assess a subset of the Corporation's common controls and privacy controls.	Closed	Agree
FY 14 - FISMA - NFR 13	**Recommendation 1:** Review and update the hardware and/or configuration of the SSL/TLS VPN device to comply with FIPS PUB 140-2- and FIPS PUB 202-approved cryptographic algorithms (i.e., 3DES, AES-128, AES-256, SHA-2, and SHA-3) and TLS 1.2.	Closed	Agree
FY 14 - FISMA - NFR 14	**Recommendation 1:** Develop a more effective and comprehensive DRP and COOP by:		
	Part A: Developing an individual BIA for each critical system with participation from the business owner based upon the BIA template format found in NIST SP 800-34, Rev. 1.	Part A: Closed	Agree
	Part B: Determining information system recovery criticality, including allowable downtime and acceptable data loss based on business process needs.	Part B: Closed	Agree
	Part C: Identifying outage impacts, resource requirements, and recovery priority for system resources.	Part C: Closed	Agree
	Part D: Updating the DRP to cover the entire Corporation and other critical IT contractors and not just the MITS contractor.	Part D: Closed	Agree
	Part E: Updating the COOP based on revisions to the BIA and DRP.	Part E: Open	Agree Modified Repeat, refer to Finding 7

Table 6: Status of Prior Year FY 2015 Recommendations

FISMA NFRs	FY 2015 FISMA Evaluation	CNCS Status	Auditor Position on Status
FY 15 - FISMA - NFR 2	**Recommendation 1:** Execute the automated script to disable inactive accounts on a nightly basis, rather than current practice of twice a month, to enforce the Corporation's policy to disable accounts that have not been accessed in the prior 30 days.	Closed	Modified Repeat, refer to Finding 3
	Recommendation 2: Implement an automated alert to notify the Corporation on a daily basis when accounts "disabled" after 30 days must be deleted. For disabled user accounts that should not be deleted, due to circumstances such as medical leave, the user account should be moved into a special AD OU that is not subject to automatic deletion (modified repeated condition from FY 2015).	Closed	Agree
FY 15 - FISMA - NFR 4	**Recommendation 3:** Perform biannual physical IT inventory audits at HQ and field offices to ensure the IT inventory list and assignments of physical IT assets are accurate.	Closed	Modified Repeat, refer to Finding 8

Table 7: Status of Prior Year FY 2016 Recommendations

FISMA NFRs	FY 2016 FISMA Evaluation	CNCS Status	Auditor Position on Status
FY16 – FISMA – NFR 1	**Recommendation 1:** Update and implement the draft CM plan to incorporate security-focused configuration management requirements from NIST SP-800 53, Rev. 4 (i.e., controls CM-1 to CM-9) and NIST SP 800-128.	Closed	Agree

FISMA NFRs	FY 2016 FISMA Evaluation	CNCS Status	Auditor Position on Status
	Recommendation 2: Establish and document the Corporation's secure configuration baseline for desktops and servers. Consider guidance from NIST SP 800-70 Rev. 3 National Checklist Program for IT Products and external sources such as Microsoft and the Center for Internet Security for the development of secure configuration baselines.	Closed	Agree
	Recommendation 3: Implement a process to maintain configuration baselines for desktops, servers and other network equipment that records installed software, software versions, and configuration settings as required by NIST SP 800-53, CM-2 Baseline Configuration.	Open	Agree Modified Repeat, refer to Finding 2
	Recommendation 4: Improve TRB CM procedures by implementing a process to document and track deviations from approved configuration baselines, as required by CM control CM-3 Configuration Change Control. As part of the process, ensure deviations from the configuration baselines are documented with business justification.	Open	Agree Modified Repeat, refer to Finding 2
	Recommendation 5: Perform periodic configuration scans to identify deviations from the Corporation's configuration baselines for desktops, servers, and network equipment. The objective of the configuration scans should be to identify deviations (i.e., missing or outdated antivirus software, missing backup agents, non-standard software or settings) from the approved configuration baseline in contrast to other scans designed to identify missing security patches and other vulnerabilities.	Open	Agree Modified Repeat, refer to Finding 2

FISMA NFRs	FY 2016 FISMA Evaluation	CNCS Status	Auditor Position on Status
FY16 – FISMA – NFR 2	**Recommendation 1:** Develop and implement a process to monitor GSS backup jobs for failures, particularly for backup jobs identified as critical. Consider utilizing automated alerts and developing naming conventions for server backup jobs identified as "critical" backups to ensure prompt, corrective action is taken by responsible individuals. Update the GSS SSP to reflect the new monitoring process for backup jobs.	Closed	Agree
	Recommendation 2: Investigate backup job failures when they continue to occur to determine the root cause and remedial solutions	Closed	Agree
	Recommendation 3: Develop a service level agreement (SLA) or performance metrics to ensure that GSS backups are performed in accordance with contractual requirements.	Open	Agree Repeat, refer to Finding 7

MANAGEMENT COMMENTS

Corporation for National and Community Service

NationalService.gov

December 8, 2017

To: Stuart Axenfeld
Assistant Inspector General for Audit

Re: Request for Comments on the Office of Inspector General's (OIG) Draft Report: Fiscal Year 2017 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service

The Corporation for National and Community Service (CNCS) has received a draft copy of the Fiscal Year (FY) 2017 Federal Information Security Modernization Act (FISMA) evaluation. While this evaluation purports to represent an independent review of the Agency's cybersecurity program, it fails to consider a number of mitigating facts and circumstances. Additionally, the FISMA evaluation fails to properly consider that a small agency like CNCS should not and cannot be held to the same level of maturity as large federal agencies and realistically only a multi-year approach to CNCS's evaluation is meaningful.

The report noted significant improvements and acknowledged that while deficiencies remain, CNCS has continued to make improvements. The FY 2017 evaluation documents that in four of the five Cybersecurity Framework areas, CNCS improved in each area by a full maturity level. This should be noted as a significant achievement. Regardless, CNCS does not believe that this evaluation sufficiently reflects the improved status of its Cybersecurity program. The evaluation has indicated 14 findings with a total of 34 recommendations. As explained in detail below, CNCS accepts 10 recommendations; partially accepts 17; and rejects the remaining 7 recommendations.

As the report noted, CNCS has devoted necessary resources to demonstrate a consistent level of improvement in Cybersecurity. CNCS remains committed to continuing to improve its Cybersecurity position, however, until the FISMA evaluation provides considerations for small agencies (and/or special Cybersecurity funding is made available), CNCS will only be able to achieve controlled improvements, as it must stay focused on preserving and strengthening those elements that protect the privacy data that it maintains. CNCS will continue to use the Plan of Actions and Milestones (POAM) as the process by which Cybersecurity corrections are tracked and managed. Over the course of the last year only one POAM item was rescheduled from its original target date, further demonstrating that the 106 POAM items that were identified last year and closed in FY 2017 are being properly managed. CNCS looks forward to continued improvement in its Cybersecurity program.

1. CNCS Must Strengthen its Organization-wide Information Security Program

Authorization to Operate (ATO)

CNCS Cybersecurity Policy states "To address the needs of constantly changing environments, CNCS shall adopt ongoing authorization (OA), which involves shifting from periodic to ongoing assessments and facilitates a continual state of awareness. As current system authorizations expire, an OA will be issued upon completion of its security assessment." Upon expiration of the eSPAN extended ATO eSPAN entered into an ongoing authorization, which included monthly review of specific NIST 800-53r4 security controls. The continuous monitoring of security controls started in June 2017 and eSPAN has provided the required evidence each month. No significant changes occurred with the eSPAN system before or after the ATO expired in June 2017. Essentially, the security posture did not change once eSPAN entered into an OA.

The statement that "…the Authorizing Official (AO) cannot be held accountable for accepting the risk to operate these systems. Further, the security posture of CNCS systems may not be at an acceptable level of risk to operate,…" is exaggerated and is not based upon facts. Using the Risk Management Framework and continuously reviewing security controls along with a weekly review and assessment of risks ensured that the overall security posture was unchanged. It should also be noted that the delay in completing the documentation was a risk based decision, based upon determining the status of the GMM launch and the desire not to devote resources to an effort that would potentially need to be redone several months later. The eSPAN security assessment will be completed no later than December 30, 2017.

Systems Security Plans

NIST 800-53A, *Assessing Security and Privacy Controls in Federal Information Systems Revision 4 and Organizations — Building Effective Assessment Plan*, does not have specific guidance for assessing Appendix J Privacy Controls. As such, beyond policies and procedures, there is not a clear method of identifying how privacy controls should be implemented and assessed. Every CNCS information system that handles privacy information has a current Privacy Impact Assessment (PIA) on file. The PIAs define what privacy information is being collected, and how it is being used and protected. Until such time that further guidance is provided for federal agencies, CNCS believes the PIA along with the Privacy Policy provides sufficient documentation to provide an acceptable level of confidence that privacy information is properly controlled. CNCS recognizes that the FY 2016 FISMA recommendation to enhance controls was not completed to the auditor's satisfaction but believes the recommendation was adequately addressed because the Chief Privacy Officer is able to substantially validate compliance with privacy controls.

System Risk Assessments

A full risk assessment was conducted on the GSS in April of 2016, and another focused risk assessment was conducted specifically on the Azure environment in February of 2017, thus covering all of GSS. The February assessment was targeted because CNCS, in compliance with the federal mandate of "Cloud First", is in the process of moving to a full cloud infrastructure. The GSS was assessed in smaller segments to allow for proper evaluation and correction of potential issues. Risks to the GSS were identified and addressed throughout the year rather than having a single all-encompassing risk assessment.

Cybersecurity provided the Momentum Security Assessment Report (SAR) that was completed in July 2017, which included all of the risk assessment elements required by NIST. Clearly, the most recent SAR was not considered when defining the criteria for this Momentum finding.

Based upon this year's FISMA evaluation, CNCS is reviewing the network architecture to fully define what information systems (including both cloud and shared services) should be considered part of the CNCS network.

Plan of Action and Milestones Process

CNCS does **not** concur with the POAM findings or accept the related recommendations for the following reasons:

- Undocumented control weaknesses from the GSS Azure assessment are on the GSS system level POAM, but a POAM addressing the need for a baseline is currently open on the corporate POAM (FY16-CNS-1.3), thus there isn't a need to duplicate information between the system and corporate level POAM.
- POAMs were intentionally not created for any of the control weaknesses documented in the eSPAN Security Assessment Report because at the time of the assessment, GMM was on schedule to replace eSPAN. CNCS management made the decisions that it was not going to expend resources to a legacy system that was being replaced. With the delayed deployment of GMM, eSPAN is scheduled for a full assessment in which control weaknesses will be tracked on the system level POAM.
- POAMs were created for the control weaknesses documented in the Momentum assessment conducted in June 2017 by VMD. CNCS is confident that the current POAM process is mature and effective given maturation of the process over the past several years. In addition to this, the Cybersecurity team conducts weekly reviews of the POAMs with the ISSOs. This information is then briefed monthly to the CISO for final concurrence and approval.

Risk Management Strategy

The Office of the Chief Risk Officer (OCRO) provided evidence that validated completion of recommendations found in related corporate level POAMs associated with previous audits and assessments. Notably, documentation regarding POAMs FY14-CNS-9.0, FY14-CNS-9.1.a, FY14-CNS-9.1.b, and FY14-CNS-9.1.c were submitted to OIT for closure of these POAMS on September, 27th 2017. The CISO is responsible for cybersecurity risk through a process of POA&Ms and ISCM to manage and identify potential vulnerabilities, and to establish risk tolerance and thresholds. Information system cybersecurity risks are conveyed as needed to the CIO and the Information Technology Steering Committee (ITSC) to allocate resources. When an identified risk impacts the entire enterprise, the CISO will convey the information to the Risk Management Council, which meets quarterly or more frequently if needed, to assess and prioritize risks and mitigation strategies that are then recommended to the CEO.

Recommendation 1 (Reject): As written, this recommendation adds no value or improvement. It is equivalent to CNCS's current practice for documenting the continuous monitoring program and security authorization process. CNCS already has processes and documentation that address the continuous monitoring program and security authorization process. CNCS has the following documentation in place:

- Cybersecurity Policy
- Information Security Continuous Monitoring (ISCM) Strategy
- IT Risk Management Framework (RMF) Guide
- Security Assessment and Authorization (SA&A) Standard Operating Procedures (SOP)

Recommendation 2 (Accept): CNCS will address this recommendation with the caveat that it will be using future NIST guidelines for defining how privacy controls should be implemented and assessed.
Recommendation 3 (Accept): CNCS will incorporate this recommendation into its existing processes.
Recommendation 4 (Partially Accept): CNCS does not have the resources to review external connections at the level described. CNCS will consider creating a cost-effective alternative process that addresses the concerns defined by this recommendation.
Recommendation 5 (Reject): CNCS has a process in place for identifying, defining, and managing POA&Ms. The recommendation does not improve or enhance CNCS's current process.
Recommendation 6 (Reject): As written, this recommendation would not improve CNCS's existing processes. Currently, the CISO has monthly meetings specifically to review and approve the closure of POA&Ms. Members of Cybersecurity meet continuously with system ISSOs and ISO to discuss the security posture of the system to include open and closed POA&Ms.
Recommendation 7 (Partially Accept): CNCS concurs conceptually with the Risk Management finding, however, portions of the recommendation have been resolved, or are in the process of being addressed as noted below:

- Finalize the risk register (resolved): The CNCS Risk Register was approved by the Risk Management Council (RMC) on 20 April 2017.
- Establish the risk tolerance for the Corporation to include information security and privacy and communicate the risk tolerance throughout the organization (in process): An initial CNCS risk appetite statement has been drafted and will be presented to the RMC for discussion during its December 2017 meeting.
- Develop, document and implement acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance (in process): The RMC developed its initial risk register in 2017, and the Enterprise Risk Management Program Manager is refining the processes that resulted in CNCS's first register to routinize the process going forward.
- Develop, document and implement approaches for monitoring risk over time (in process): The RMC is in the process of approving risk mitigation strategies for its first risk register and will routinize the process going forward.

2. CNCS Needs to Improve its Configuration Management Controls

Standard Baseline Configurations

CNCS has an open POA&M item related to establishing a baseline configuration for all devices that are part of the CNCS network. The scheduled completion date for that POA&M was Oct 31, 2017; since the time of this report, the POA&M has been closed. Between now and the end of January 2018, CNCS intends to document the deviations from the baseline and ensure all devices are configured accordingly.

System Change Controls

- CNCS has taken steps to make sure SIA's are completed when necessary. An SIA is completed to document the security impact of a change, not to determine if there is a security impact. The SIA SOP lists all possible changes that would require a SIA and is referenced in the Configuration Management SOP.
- CNCS will update the SIA SOP to reflect how to use the SIA questionnaire to assist in identifying the need to complete an SIA.

- CNCS will also add an SIA checkbox to items presented before the Technical review board to ensure documentation of a determination of security impact and ensure that follow-on steps are conducted, when necessary.
- Even though this information was not formally documented, this process was part of the ISSO role based training conducted in October 2016. CNCS will consider improving its documentation of this process.

Recommendation 8 (Accept): CNCS already has an open POA&M related to this recommendation.
Recommendation 9 (Reject): The process for defining what changes require an SIA are defined in the SIA SOP. Those responsible for developing an SIA are fully aware of when the SIA is required. The FISMA evaluation appears to have misunderstood the SIA SOP.

3. CNCS Needs to Strengthen Account Management Controls

Access Approval

The only privileged user that was identified as not having a signed privileged user rules of behavior was due to administrative oversight. This oversight would have been found and corrected during the annual training. This administrative oversight does not imply that policies are not enforced; in fact, it reflects consistent enforcement with the occasional human error resulting from the fact that currently, the privileged account management is a manual process. However, because all privileged user complete annual training and re-sign their privileged user rules of behavior, such oversight mistakes are caught and corrected in a timely manner.

Account Recertification

No additional comment

Separated Users

No additional comment

Inactive Accounts

CNCS will consider reviewing the account management process for all systems and identify ways to improve the validation of accounts using the resources currently available.

Recommendation 10 (Partially Accept): A process already exists that requires privileged users to complete privileged user training and sign the privileged user rules of behavior. CNCS will consider whether it is cost effective to implement a periodic check of privileged users to ensure all identified privileged users have completed the rules of behavior.

Recommendation 11 (Reject): CNCS already has a process for verifying eSPAN related accounts. The verification processes has been successfully completed for the last two quarters. There was a lapse in this process because a staff member unexpectedly died and some of the responsibilities of the deceased were not immediately reassigned.

Recommendation 12 (Partially Accept): CNCS has an account management policy in place. The recommendation as written would require CNCS to expend far more resources than are available for managing accounts. The current process will be reviewed to see where improvements can be made using existing tools and available resources.

Recommendation 13 (Partially Accept): CNCS has processes in place that automatically disable user accounts after 30 days of inactivity. A review of these disabled accounts occurs on a monthly basis. This review process is manual and relies upon other CNCS offices completing their portions of the on-boarding or off-boarding process. CNCS will consider exploring other options to streamline this process.

4. CNCS Must Implement Multifactor Authentication for Privileged and Non-Privileged Accounts

   CNCS has an existing open POAM related to this finding (FY16-CNS-14) and an approved project to address implementing multifactor authentication for network access for privileged users. Higher priority projects and lack of funding delayed implementation of multifactor authentication for network access for privileged users in FY17. CNCS is aware of this deficiency and hopes to make it a priority in FY 18.

   Recommendation 14 (Accept): CNCS already has a project planned to implement multifactor authentication for privileged users.

   Recommendation 15 (Accept): As resources become available, CNCS will work towards implementing multifactor authentication on the CNCS network.

5. CNCS Needs to Enhance the Review and Analysis of Momentum Audit Logs

   This was a known issue that was tracked as a Corporate level POAM item, FY16-CNS-2.5. At the time of the FY 17 FISMA Audit, CNCS was scanning one Oracle database to test the tool and related process. A complete roll out of database scanning was deferred while the Network team was troubleshooting network latency issues. With successful testing and network issues resolved, 16 additional database servers have been incorporated into to the weekly scan list, as of September 10, 2017.

   Additionally, since this server resides in a FedRAMP authorized environment, a portion of the security controls are inherited from that facility service provider. However, this has brought to light the need to review the classification of Momentum, which as defined in the NIST 800-144, meets the criteria as a Software-as-a-Service. CNCS will review the Momentum system in the future.

   Recommendation 16 (Accept): CNCS is actively working to ingest Momentum log into the log aggregation tool Splunk.

   Recommendation 17 (Partially Accept): As CNCS reviews the system classification and usage of Momentum this recommendation will be considered and may be accepted entirely.

6. CNCS Needs to Enhance the Personnel Screening Process

   At the time when the sample employees were on-boarded, the Personnel Security office only sponsored employees for NACI investigations. Since then, OPM has made a Position Designation Tool (https://www.opm.gov/investigations/suitability-executive-agent/position-designation-tool/#url=Overview) available to assign risk/sensitivity to a position and identify the required investigation level.

   Recommendation 18 (Accept): The Office of Human Capital (OHC) is currently re-designating all agency positions (federal employees and contractors), and the Personnel Security office is ensuring employees in those positions have the necessary level of investigation and sponsoring employees who do not.

   Recommendation 19 (Accept): OHC currently documenting the process for validation background investigation are commensurate with the level of the position.

7. CNCS Needs to Strengthen Contingency Planning Controls

Recommendation 20 (Partially Accept): CNCS will consider developing a formal means of capturing the results of any GSS/eSPAN disaster recovery test. Given CNCS's limited resources, ensuring lessons learned are documented and reviewed and corrective action taken will have to be prioritized with other relevant operational requirements.

Recommendation 21 (Reject): This is an existing POA&M with a scheduled completion date of December 31st , 2017.

Recommendation 22 (Reject): This is recommendation is currently managed using the existing POA&M process. The current schedule for addressing this specific POA&M is December 2017.

The following findings are a result of field office visits.

8. CNCS Needs to Consistently Enforce an Agency-wide Information Security Program Across the Enterprise

Recommendation 23 (Accept): CNCS agrees that management of field sites need to be evaluated and looks forward to improving controls and performance monitoring at all field site. CNCS will review this recommendation further to determine the future direction of managing CNCS field sites information security.

9. CNCS Must Improve its Vulnerability and Patch Management Controls

Recommendation 24 (Partially Accept): CNCS continues to operate an effective patch management process at headquarters, but acknowledges that it needs to better apply those procedures to the field sites to ensure remote devices are also being properly patched and incorporated into the POAM process, if necessary. CNCS intends to review how field sites are currently managed and devise a plan that works across all entities of CNCS.

10. CNCS Needs to Strengthen Access Controls for Mobile Devices

Recommendation 25 (Partially Accept): CNCS has identified that management of mobile devices at field sites needs to be evaluated considering the advances in technology and the changing needs of field site employees. This finding will be reviewed to determine if it aligns with the future direction of managing CNCS field sites.

Recommendation 26 (Partially Accept): CNCS will consider the recommendation as it examines at a higher level the current management of mobile devices in field sites.

Recommendation 27 (Partially Accept): CNCS will consider the recommendation as it examines at a higher level the current management of mobile devices and field sites.

11. CNCS Needs to Strengthen Monitoring of Wireless Access Connections

Recommendation 28 (Partially Accept): CNCS will consider the recommendation as it examines the wireless access needs of the field offices.

Recommendation 29 (Partially Accept): CNCS will consider whether restricting the use of the FEMA wireless network at NCCC campuses is practical, feasible, and improves efficiencies.

12. CNCS Needs to Strengthen the Protection of Personally Identifiable Information

    Recommendation 30 (Partially Accept): CNCS will review the current process of who has access to files in the storage room and determine if additional monitoring controls are necessary and feasible.

13. CNCS Needs to Improve the Information Technology Asset Inventory Management Process

    Recommendation 31 (Partially Accept): CNCS will review and consider implementing improved procedures for reconciling the accuracy and completeness of the FasseTrack system.

14. CNCS Needs to Improve Physical and Environmental Protection Controls

    Recommendation 32 (Partially Accept): CNCS will consider developing a feasible process of reviewing video recordings and monitoring camera feeds at the Vicksburg NCCC campus.

    Recommendation 33 (Accept): CNCS has taken the necessary steps to ensure all of the field sites have fully operational UPS and will be issuing specific guidance on what should happen in case of an UPS failure.

    Recommendation 34 (Partially Accept): CNCS will consider reviewing the safety parameters at the Jackson State Office and take reasonable corrective actions.

Digitally signed by ANDREA SIMPSON
DN: c=US, o=U.S. Government, ou=Corporation for National and Community Service, cn=ANDREA SIMPSON, 0.9.2342.19200300.100.1.1=95771002878969
Date: 2017.12.11 11:52:01 -05'00'

Andrea Simpson
Chief Information Security Officer / Director of Cybersecurity
Office of Information Technology (OIT)
Corporation for National and Community Service (CNCS)

OFFICE OF INSPECTOR GENERAL

CORPORATION FOR

NATIONAL & COMMUNITY SERVICE

CORPORATION FOR NATIONAL & COMMUNITY SERVICE
250 E ST SW, WASHINGTON, DC 20024
202.606.5000 | WWW.NATIONALSERVICE.GOV/

OFFICE OF INSPECTOR GENERAL
HOTLINE: 1.800.452.8210
HOTLINE@CNCSOIG.GOV | WWW.CNCSOIG.GOV/