CORPORATION FOR NATIONAL & COMMUNITY SERVICE

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2018 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG Report 19-03

Prepared by:

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

This report was issued to Corporation management on March 1, 2019. 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 September 3, 2019, and complete its corrective actions by March 2, 2020. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

OFFICE OF INSPECTOR GENERAL
CORPORATION FOR
NATIONAL & COMMUNITY SERVICE

March 1, 2019

MEMORANDUM TO: Barbara Stewart
Chief Executive Officer

Dr. Pape Cissé
Chief Information Officer

FROM: Monique P. Colter /s/
Assistant Inspector General for Audit

SUBJECT: Fiscal Year 2018 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service (OIG Report 19-03)

Attached is the final report on the Office of Inspector General's (OIG) Report 19-03, *Fiscal Year 2018 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.

Under the Corporation for National and Community Service's audit resolution policy, a final management decision on the findings and recommendations in this report is due by September 3, 2019. Notice of final action is due by March 2, 2020.

Should you have any questions about this report, please contact me at 202-606-9360.

Enclosure:
As stated

cc: Desiree Tucker-Sorini, Chief of Staff
Timothy Noelker, General Counsel
Edward (Woody) Davis Jr., Deputy Chief Information Officer
Andrea Simpson, Chief Information Security Officer
Lori Giblin, Chief Risk Officer
Robert McCarty, Chief Financial Officer
Lora Pollari-Welbes, Audits and Investigations Program Manager
Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

CliftonLarsonAllen

Fiscal Year 2018 Federal Information Security Modernization Act Evaluation for the Corporation for National and Community Service

March 1, 2019

Final Report

CLA (CliftonLarsonAllen LLP)
901 North Glebe Road, Suite 200
Arlington, VA 22203-1853
571-227-9500 | fax 571-227-9552
CLAconnect.com

March 1, 2019

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

Dear Ms. Stewart:

The Federal Information Security Modernization Act of 2014 (FISMA) requires each Inspector General to assess annually the effectiveness of the information security program at that Inspector General's agency. The Office of Inspector General for the Corporation for National and Community Service (CNCS-OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the FISMA evaluation for Fiscal Year 2018.

We have determined that the Corporation for National and Community Service's (CNCS's) information security program is **NOT EFFECTIVE**. Two approaches reach this conclusion: (1) the Federal government-wide objective metrics used by all Inspectors General and prescribed by the Department of Homeland Security, which grade cybersecurity programs on a maturity scale from Level 1 (*Ad Hoc*) to Level 5 (*Optimized*); and (2) our judgmental assessment of the information security and privacy program, practices and controls for select systems. Overall, CNCS made small gains from last year in certain components of its program, but those improvements did not move CNCS's information security program substantially closer to an Effective level, especially relative to the resources invested.

CNCS has in place the basic information technology policies, procedures and system security documentation needed for effective cybersecurity. In other words, the simple work is done. To progress beyond the current maturity level, the Corporation must consistently implement and monitor security controls. We continued to find severe vulnerabilities on the network, and CNCS has still not fully implemented baseline security configuration settings specific to the existing information technology environment. Further, CNCS has still not implemented multifactor authentication for information system users and administrators. These gaps limit the protection of CNCS systems and data and may expose sensitive information, including Personally Identifiable Information (PII), to unauthorized access and use.

To date, CNCS's approach to information security and privacy has been reactive, rather than strategic. The Corporation has invested time and effort to remedy specific gaps but has not developed a strategic approach that will ultimately achieve effective cybersecurity. Thus, the recent efforts have not produced commensurate progress.

Among other recommendations, we strongly urge that CNCS reverse-engineer the government-wide maturity model and treat it as a roadmap. CNCS should undertake a strategic analysis of the government-wide metrics and the weaknesses identified in this evaluation, to develop a multi-year approach designed to realize steady, measurable improvements in information security in each of the component areas. Implementing such a plan will require CNCS to allocate sufficient resources, including staffing, and to be accountable for interim milestones, in order to reach an overall Effective rating within a reasonable period to be specified by management, *e.g.*, two to three years.

We appreciate the assistance we received from CNCS and hope that our evaluation and recommendations are helpful. 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 1

Summary of Results 6

FISMA Evaluation Findings 11

Security Function: Identify 11

1. CNCS Must Improve its Vulnerability and Patch Management Controls 11
2. CNCS Must Maintain the Security Authorization Process in Accordance with OMB and NIST Requirements 13
3. CNCS Must Fully Implement its Risk Management Program 14

Security Function: Protect 18

4. CNCS Must Improve its Configuration Management Controls 18
5. CNCS Must Implement Multifactor Authentication for Privileged and Non-Privileged Accounts 20
6. CNCS Must Strengthen Account Management Controls 21
7. CNCS Must Enhance the Personnel Screening Process 22
8. CNCS Must Improve Physical Access Controls 24

Security Function: Detect 27

9. CNCS Must Enhance the Review and Analysis of Momentum Audit Logs 27

Appendix I – Scope and Methodology 31

Appendix II – Status of Prior Year Recommendations 34

Appendix III – Independent Assessor Evaluation 47

Appendix IV – Management Comments 48

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 540 employees and approximately 130 contractors 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.

Overview of CNCS Information Technology Systems and Governance

CNCS relies on information technology (IT) systems to accomplish its mission of making grants and managing a residential national service program. The Corporation has a Federal Information Security Modernization Act of 2014 (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 Financial Management System (Momentum), AmeriCorps Health Benefits, AmeriCorps Childcare Benefits System, and public websites.[1] The first five of these systems are categorized as moderate security, while the public websites are rated as low security.[2] All six systems are hosted and operated by third-party service providers, although the Corporation hosts certain components of the GSS. The Corporation's network consists of multiple sites: Headquarters (HQ), one Field Financial Management Center (FFMC), four National Civilian Community Corps (NCCC) campuses, and more than 50 AmeriCorps state offices throughout the United States. These facilities are connected through commercially managed telecommunications network connections.

In July 2018, CNCS closed the Baltimore, Maryland NCCC campus and relocated a majority of its information technology assets to the Washington D.C. headquarters (HQ) and the remaining four NCCC campuses. Additionally, CNCS relocated the Volunteers in Service to America (VISTA) Member Support Unit (VMSU) from Austin, Texas to the HQ in January 2018.

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. Despite this, CNCS by law retains responsibility for complying with the requirements of the FISMA and security control implementation.

[1] 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 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.

[2] The Federal Information Processing Standards 199, *Standards for Security Categorization of Federal Information and Information Systems*, (Feb. 2004), determine the security category (*i.e.*, low, moderate, high) of a Federal information system based on its 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. 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 grantmaking: 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.

CNCS 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 Acting Chief Information Officer (ACIO) leads the OIT and the Corporation's IT operations. The ACIO 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

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 sources.

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 General (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 FIPS to establish agency baseline security requirements.

FY 2018 IG FISMA Reporting Metrics

OMB and the Department of Homeland Security (DHS) provide annual instructions to Federal agencies and IGs for preparing FISMA reports. On October 16, 2017, OMB issued Memorandum M-18-02, *Fiscal Year 2017-2018 Guidance on Federal Information Security and Privacy Management Requirements*. The memorandum establishes information security priorities and provides agencies with FY 2017-2018 FISMA and Privacy Management reporting guidance and deadlines. We performed our independent assessment according to the FISMA reporting metrics prescribed for Inspectors General for FY 2018.[3]

The FY 2018 IG FISMA Reporting Metrics (IG FISMA Metrics) incorporate a maturity model that aligns with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.0: Identify, Protect, Detect, Respond and Recover.[4] 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 2018 IG FISMA Metric Domains

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring

[3] https://www.dhs.gov/publication/fy18-fisma-documents
[4] Data Protection and Privacy was added to the FY 2018 metrics in the Protect security function.

Cybersecurity Framework Security Functions	FY 2018 IG FISMA Metric Domains
Respond	Incident Response
Recover	Contingency Planning

The lower (foundational) levels of the maturity model focus on the development of sound, risk-based policies and procedures, while the advanced levels leverage automation and near real-time monitoring in order to achieve the institutionalization and effectiveness of those policies and procedures. **Table 2** explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of at least Level 4, *Managed and Measurable*.

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.[5] In addition, the evaluation included inquiries, observations, inspection of documents and records, and testing of controls.

[5] https://www.ignet.gov/sites/default/files/files/committees/inspect-eval/iestds12r.pdf

For this evaluation, we reviewed selected management, operational, and technical controls in accordance with NIST 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 (FFMC and one NCCC campus and State Office). In addition, our evaluation included an assessment of effectiveness for each of the eight FY 2018 IG FISMA Metric Domains[6] and the maturity level of the five Cybersecurity Framework Security Functions. See Appendix I for the detailed scope and methodology.

[6] https://www.dhs.gov/sites/default/files/publications/Final%20FY%202018%20IG%20FISMA%20Metrics%20v1.0.1.pdf

SUMMARY OF RESULTS

CNCS's information security program is **Not Effective.** Whether assessed objectively under the maturity model in the IG FISMA Metrics[7] or the NIST baseline criteria applied judgmentally by the evaluators, the result is the same.

The Corporation implemented more than half of the outstanding prior recommendations and made small gains in certain components of the IG FISMA Metrics maturity model and its overall security program. However, that progress was not significant enough to move CNCS's information security program substantially closer to an Effective level as a whole, especially relative to the resources invested.

Over the past few years, CNCS has developed information technology policies, procedures, and system security documentation. These are necessary and foundational cybersecurity steps. However, to achieve effective information security, CNCS must progress to consistent implementation and monitoring of security controls. For example, our evaluation continued to find significant vulnerabilities on the network, and CNCS has still not fully implemented baseline security configuration settings specific to the Corporation's information technology environment. The lack of properly implemented baseline configuration settings reduces the effectiveness of enterprise security controls for protecting CNCS systems and data. This may expose sensitive information, including Personally Identifiable Information (PII), to unauthorized access and use.

We submit 25 new or modified recommendations to assist CNCS in strengthening its information security program. Most importantly, we recommend that CNCS use the IG FISMA Metrics to develop a strategic plan designed to accomplish steady and measurable progress towards an Effective level in each of the five functional areas specified in the CSF. Addressing the effectiveness of the information security program requires a comprehensive strategy and solution of people, processes and technology. Implementing such a plan will require CNCS to allocate sufficient resources, including staffing, and to be accountable for interim milestones, in order to reach an overall Effective rating within a reasonable period to be specified by management.

Progress since FY 2017

CNCS has devoted significant resources to improving its information security program and practices over the past few years. Specifically, since last year it closed 24 out of 45 open recommendations from the FY 2014 – FY 2017 FISMA evaluations.[8] As a result, the Corporation has made improvements in the following areas:

- Enforced the Corporation's account management procedures for disabling inactive accounts and performing account recertification.

- Enhanced the Plan of Action and Milestone (POA&M) management process to ensure all known security control weaknesses are tracked for remediation.

[7] OMB Memorandum 18-02 requires evaluators across the Federal government to respond in the DHS CyberScope system to 67 objective questions, from which an DHS algorithm calculates a maturity score for each of five CSF function areas. https://www.whitehouse.gov/sites/whitehouse.gov/files/omb/memoranda/2017/M-18-02%20%28final%29.pdf

[8] The prior FISMA evaluations from FY 2014 to FY 2016 were performed by another CPA firm.

- Documented the Corporation's risk tolerance, and an enterprise risk management plan that addresses risk assessment methodologies and mitigation strategies, and a process for evaluating and monitoring risk across the agency.

- Updated the Continuity of Operations Plan (COOP) based on revisions to the Business Impact Analysis (BIA) and Disaster Recovery Plan (DRP)

As of the close of fieldwork, however, CNCS had not completed corrective actions for 21 prior recommendations. One of them dated back to the FY 2014 FISMA evaluation and three recommendations dated back to FY 2016 FISMA evaluation.

Current Status

Despite the noted progress, the Corporation's efforts have focused on developing policies and procedures and system security documentation, but have stopped short of consistent implementation and monitoring of security controls. For example, CNCS implemented a process to scan the Corporation's network and critical applications for vulnerabilities. However, we continued to identify significant network issues, exposing the Corporation to critical and high severity vulnerabilities. We also found again this year that CNCS has not fully implemented baseline security configuration settings specific to the Corporation's information technology environment. The lack of properly implemented baseline configuration settings reduces the effectiveness of security controls for protecting CNCS systems and data. Further, CNCS has still not implemented multifactor authentication for information system users. As a result, the Corporation may be exposed to inappropriate or unauthorized access to sensitive information, including PII.

Our evaluation also identified weaknesses in organization-wide and information system risk management, security authorization documentation, system change controls, account management, personnel screening, physical access controls, and logging and monitoring controls. The weaknesses noted are associated with the IG FISMA Metric Domains: Risk Management, Configuration Management, Identity and Access Management and Information Security Continuous Monitoring.

The IG Metrics: Approach and Results

The IG FISMA Metrics prescribed for assessing the effectiveness of information security programs across the Federal government consists of 67 objective questions divided into eight "domains," which correspond to five "security functions." Based on the answers, a weighted algorithm contained in the DHS CyberScope system calculates a maturity score for each domain and security function, and then further rates the maturity of an agency's information security program as a whole. The assessment grades maturity on a scale from Level 1 (*Ad hoc*) to Level 5 (*Optimized*). A component must be rated at Level 4 (*Managed and Measurable*) to be considered Effective.

The IG FISMA Metrics maturity model is a DHS and OMB mandated tool for determining FISMA compliance. It recognizes that there are multiple stages of an information security program, and that an agency may be further along in some elements than in others. The maturity model: (1) assesses progress from year to year; and (2) helps IT professionals decide what steps are needed to reach the next level.

As set forth in the first three columns in **Table 3** below, CNCS was rated at maturity Level 2, *Defined*, in three of the five security functions, and at Level 3, *Consistently Implemented*, in the remaining two functions. Overall, the algorithm determined that CNCS's information security program was at Level 3 (*Consistently Implemented*). This rating signifies that "Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking."[9] The program falls below the Level 4 (*Managed and Measurable*) threshold for effectiveness.

Table 3 below summarizes CNCS's maturity scores in FY 2018 and compares them to the results of the FY 2017 evaluation. As shown, CNCS advanced from maturity level 2, *Defined,* to level 3, *Consistently Implemented,* for the Recover function, and from level 3, *Consistently Implemented*, to level 4, *Managed and Measurable*, for the Security Training domain in the Protect function. However, CNCS stayed at the same maturity level 2 for the Identify, Protect, and Detect functions and at level 3 for the Respond function. Although some improvement was made, the overall progress was minimal in advancing the Corporation's information security program to an effective level.

Table 3: Comparison of Maturity Ratings in FY 2018 and FY 2017

Security Function[10]	Maturity Level by Function FY 2017	Maturity Level by Function FY 2018	IG FISMA Metric Domains	Maturity Level by Domain FY 2017	Maturity Level by Domain FY 2018
Identify	Defined (Level 2)	Defined (Level 2)	**Risk Management**	Defined (Level 2)	Defined (Level 2)
Protect	Defined[11] (Level 2)	Defined[12] (Level 2)	**Configuration Management**	Defined (Level 2)	Defined (Level 2)
			Identity and Access Management	Defined (Level 2)	Defined (Level 2)
			Data Protection and Privacy	Not Included in FY 2017	Consistently Implemented (Level 3)
			Security Training	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)
Detect	Defined (Level 2)	Defined (Level 2)	**Information Security Continuous Monitoring**	Defined (Level 2)	Defined (Level 2)
Respond	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	**Incident Response**	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	Defined (Level 2)	Consistently Implemented (Level 3)	**Contingency Planning**	Defined (Level 2)	Consistently Implemented (Level 3)

[9] FY 2018 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics Version 1.0.1, May 24, 2018.

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

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

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

The IG FISMA Metrics provide a useful roadmap of the steps necessary to progress to the next level of maturity. Although CNCS made some improvements in strengthening information security controls aligned with the IG FISMA Metrics, CNCS's approach to improving its overall security program did not include an analysis of the metrics or a multi-year strategic plan targeted at increasing its individual or aggregate maturity scores. In addition, the findings identified in this evaluation align with the particular security domains,[13] but we caution that remedying those weaknesses alone may not increase the related maturity scores. CNCS should use the IG FISMA Metrics to prioritize, target its efforts, and allocate resources most effectively.

Judgmental Assessment: Approach and Results

The annual IG FISMA Metrics assessment may, but is not required to, include a subjective, judgmental assessment of an agency's information security program. The judgmental assessment sometimes differs from the IG metrics scores as the judgmental assessment may take into account the results of controls tested during the independent evaluation and an analysis of risk for control weaknesses.

Like the maturity model, our judgmental assessment determined that CNCS's information security program is **Not Effective**, overall and for each of the five security functions. However, we rated certain individual elements (domains) within those functions more highly than did the CyberScope algorithm. In particular, we found it to be effective in four of the individual domains: Data Protection and Privacy, Security Training, Incident Response and Contingency Planning. **Table 10** in **Appendix III** provides a graphical overview of our judgmental assessment.

The difference is because the judgmental assessment used standards that are less demanding than the IG FISMA Metrics. The subjective assessment measured operating effectiveness under the minimum security control baselines defined by the 2013 NIST SP-800 53, Revision 4; by design, the IG FISMA Metrics contain additional requirements. In effect, the judgmental assessment was graded on a lower curve, so it awarded CNCS a higher grade. The maturity model and the IG FISMA Metrics, which are newer, are intended to set a higher standard.

Table 4 summarizes our detailed findings from our evaluation, grouped by the Cybersecurity Framework Security Functions. Also included with the FISMA Evaluation Findings in the body of this report is a discussion of the maturity model scoring for each function area.

Table 4: Findings Noted During the FY 2018 FISMA Evaluation of CNCS

IG FISMA Metric Domain	Enterprise Level Findings	Facility Level Findings
Risk Management	Unpatched and unsupported software **(Finding 1)**	Unpatched and unsupported software **(Finding 1)**
	Lack of transferred responsibility, accountability, and risk acceptance to new Authorizing Official **(Finding 2)**	
	Lack of a mission and business risk registry **(Finding 3)**	
	Incomplete information system risk assessments **(Finding 3)**	

[13] See table 4

IG FISMA Metric Domain	Enterprise Level Findings	Facility Level Findings
	Lack of assessing information technology risk to the Corporation associated with the use of external information systems **(Finding 3)**	
Configuration Management	Configuration baselines not fully implemented **(Finding 4)**	
	Incomplete or undocumented system change testing **(Finding 4)**	
	Lack of documented baseline configuration deviations **(Finding 4)**	
Identity and Access Management	Lack of multifactor authentication **(Finding 5)**	Inadequate physical controls **(Finding 8)**
	Insufficient account management controls **(Finding 6)**	
	Insufficient personnel screening process **(Finding 7)**	
Information Security Continuous Monitoring	Inadequate review and analysis of audit logs **(Finding 9)**	

Management's Response and Evaluator's Comments

In response to the draft report, CNCS concurred with 23 recommendations and did not concur with two recommendations.

Of the 23 recommendations CNCS concurred with, we noted CNCS had either taken corrective actions or planned actions. Based on our evaluation, management planned actions are responsive to the 23 recommendations. These recommendations will remain open until the OIG can validate the implementation of these actions.

Management did not concur with Recommendations 4 and 19. Recommendation 4 is related to the risk register at the mission and business process level. For Recommendation 4, management stated that the Enterprise Risk Register was created by identifying and assessing risk at the business process level as well as the enterprise level, which was provided to us. We acknowledge CNCS provided the risk register, but it was after the completion of fieldwork and there was not sufficient time to review. The risk register will be reviewed in connection with assessing the agency's corrective actions in FY 2019.

Management agreed with the finding that they must improve physical access controls to facilities. However, they disagreed to recommendation 19, which is related to monitoring camera feeds at the NCCC Vinton campus. For Recommendation 19, management stated that CNCS did not have the resources to have video cameras for all field sites nor provide dedicated security guards to monitor video feeds. In Recommendation 20, they stated that they will attempt to schedule a physical security risk assessment at NCCC campuses that had not previously had a Federal Protective Service (FPS) assessment. Management further stated that a risk acceptance for security control PE-6(1) was approved by the CNCS Risk Management Council for this security control. We will evaluate the risk acceptance during the FY 2019 FISMA Evaluation.

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

FISMA Evaluation Findings

Security Function: Identify

1. CNCS Must Improve its Vulnerability and Patch Management Controls

FY 18 IG FISMA 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 software, unsupported software, and improper configuration settings exposed the CNCS network to critical and high severity vulnerabilities. Specifically, we noted the following patch management issues:

- Based on independent scans of 14 computing devices, using the Tenable Nessus Vulnerability Scanner software tool, we identified **117 critical and 290 high risk vulnerabilities** related to patch management, configuration management, and unsupported software at the FFMC in Philadelphia, PA. Of the 407 total critical and high vulnerabilities, 355 were caused by missing patches, 29 were caused by configuration weaknesses, and 23 were caused by unsupported software. The FFMC is a high risk location for computing resources as FFMC staff monitor and manage CNCS grant funds.

- From a scan of 14 computing devices at the NCCC campus at Vinton, Iowa, we identified **24 critical and 240 high risk vulnerabilities** related to patch management, configuration management, and unsupported software. Of the 264 total critical and high vulnerabilities, 214 were caused by missing patches, 31 were caused by configuration weaknesses, and 19 were caused by unsupported software.

- From a scan of 14 servers and 306 workstations at the CNCS Washington, D.C. headquarters, we identified **1,649 critical and 6,412 high risk vulnerabilities** related to patch management, configuration management, and unsupported software. Of the 8,061 total critical and high vulnerabilities, 6,924 were caused by missing patches, 665 were caused by configuration weaknesses, and 472 were caused by unsupported software.

- From the scans at all locations, 79% of the patch management vulnerabilities were publicly known before 2017, such as those related to Adobe Acrobat, Adobe Flash Player, and Oracle. In addition, 76% of the configuration weaknesses were related to misconfigured Server Message Block and insecure library loading.

- The unsupported software was related to the following:
  - Adobe Acrobat (no longer supported as of October 15, 2017) was identified at all three locations.
  - Adobe Photoshop (no longer supported as of June 1, 2014) was identified at all three locations.
  - Microsoft XML Parser and XML Core Services (no longer supported as of April 12, 2014) was identified at the FFMC and CNCS headquarters.

- Additionally, there was an active legacy teleconferencing system which operated on an embedded unsupported Windows XP operating system at the FFMC which OIT did not know was operating on the network. Management was not aware this system was still in use as it was not being tracked on the inventory.

The overall deployment of vendor patches and system upgrades to mitigate the vulnerabilities was decentralized, inconsistent, and not effective across all facilities. In addition, the General Support System (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. In addition, the internet bandwidth available to FFMC and Vinton NCCC was not sufficient enough to allow for patches to be installed.

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.

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)
- Identifying, reporting and correcting information system flaws

The information technology systems at FFMC, Vinton NCCC campus, and CNCS Headquarters 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 FFMC, Vinton NCCC campus, and CNCS Headquarters applications. In addition, software with missing or outdated security patches could leave security weaknesses exposed to increased attack methods that compromise the confidentiality, integrity and availability of data.

To assist CNCS in strengthening vulnerability management controls, we recommend CNCS:

> ***Recommendation 1:*** *Ensure that OIT monitors and promptly install patches and antivirus updates across the enterprise when they are available from the vendor. Enhancements should include:*
>
> - *Implement a process to track patching of network devices and servers by the defined risk based patch timelines in CNCS policy. (Modified Repeat)*[14] *(FY18 – FISMA – NFR 6)*
> - *Ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer. (Repeat) (FY18 – FISMA – NFR 6)*
> - *Monitor and record actions taken by the contractor to ensure vulnerability remediation for network devices and servers is addressed or the exposure to unpatchable vulnerabilities is minimized. (Modified Repeat) (FY18 – FISMA – NFR 6)*
> - *Enhance the inventory process to ensure all devices are properly identified and monitored. (Modified Repeat) (FY18 – FISMA – NFR 6)*
>
> ***Recommendation 2:*** *Ensure that OIT evaluates if the internet connections at the Field Financial Management Center, National Civilian Community Corps Campuses, and State Office is sufficient to allow patches to be deployed to all devices within the defined risk based patch timeline in CNCS policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections. (New) (FY18 – FISMA – NFR 6)*

2. CNCS Must Maintain the Security Authorization Process in Accordance with OMB and NIST Requirements

FY 18 IG FISMA Metric Area: *Risk Management*

An Authorizing Official (AO) is a senior federal official or executive with the authority to formally assume responsibility for operating an information system at an acceptable level of risk. If the AO determines that the risk to organizational operations and assets, individuals, other organizations, and the nation is acceptable, an authorization to operate is issued for the information system. The AO is accountable for the security risks associated with information system.

The new AO for the Corporation's GSS did not sign a new authorization decision document when starting the role as the AO. Upon review of the current authorization decision document, authorization package and updated documents related to continuous monitoring activities, the new AO did not explicitly accept the known risk and formally transfer responsibility and accountability for the GSS.

[14] Modified Repeat means part of the condition, cause, or recommendation have changed from the prior year finding due to some progress made by CNCS. Repeat means there is no change to the condition, cause, or recommendation due to very limited or no progress made by CNCS.

In December 2017 when there was a change of the GSS AO, the new AO monitored the security state of the GSS through the continuous monitoring program. However, the new AO did not sign a new authorization decision document in December 2017. The new GSS AO signed a new ATO on September 11, 2018 after we brought the attention to the CISO.

OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, states: "In the event that there is a change in authorizing officials, the new authorizing official reviews the current authorization decision document, authorization package, and any updated documents created as a result of the continuous monitoring activities. If the new authorizing official is willing to accept the currently documented risk, then the official signs a new authorization decision document, thus formally transferring responsibility and accountability for the information system or the common controls and explicitly accepting the risk. If the new authorizing official is not willing to accept the previous authorization results (including the identified risk), a reauthorization action may need to be initiated or the new authorizing official may instead establish new terms and conditions for continuing the original authorization, but not extend the original authorization termination date."

Additionally, NIST SP 800-37, *Guide for Applying the Risk Management Framework to Federal Information Systems,* Feb. 2010, p. 2, n.10, 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." Appendix F, Section 5 of NIST SP 800-37 addresses reauthorization decisions and states that they "can be either time driven or event driven." In addition, the NIST *Supplemental Guidance on Ongoing Authorization,* June 2014, p. 5, states that "event–driven triggers" include "a change in the authorizing official."

Without CNCS information systems properly authorized to operate, there is no CNCS staff accountable to accept the identified risks, and be held responsible for the information system.

To assist CNCS in strengthening the security authorization process, we recommend CNCS:

> ***Recommendation 3:*** *Ensure the Chief Information Security Officer validates the security authorization process is maintained in accordance with OMB and NIST requirements. (New) (FY18 – FISMA – NFR 1)*

3. CNCS Must Fully Implement its Risk Management Program

FY 18 IG FISMA Metric Area: *Risk Management*

Risk management is the program and processes to manage risks that could affect achieving the organization's mission and objectives. An organization-wide risk management strategy includes a process for evaluating risk across the organization. NIST specifies an integrated three-tiered approach to risk management that addresses risk at the organization level, mission and business process level, and information system level.[15]

[15] NIST Special Publication 800-39, Revision 1, *Managing Information Security Risk Organization, Mission, and Information System View* specifies an integrated risk management process three-tiered approach for managing risk across an organization that "addresses risk at the: (i) organization level; (ii) mission/business process level; and (iii) information system level. The risk management process is carried out seamlessly across the three tiers with the overall objective of continuous improvement in the organization's risk-related activities and effective inter-tier and

Organization-wide Risk Management Program

The Corporation did not develop a risk register to record identified risks at the mission and business process level, or Tier 2, as defined by NIST. Additionally, although the risk register at the information system level, Tier 3, has been incorporated into the information system risk assessment and plan of action and milestone process, the information system level risk assessments for the GSS, eSPAN and Momentum did not address the following two risk management elements required by NIST:

- Likelihood[16]
- Impact analysis[17]

CNCS indicated that the Office of the Chief Risk Officer (OCRO) gathered risk information from all of the Corporation's offices to support the enterprise level risk register. However, OCRO had not started the process to document risk registers at the mission and business process (Tier 2). Without fully completed risk registers at the mission business process level, CNCS managers may not have a comprehensive understanding of the risks associated with the business processes that support the Corporation's mission and the methods for risk mitigation. As a result, CNCS's senior management (including the Chief Risk Officer) may not have the necessary information to make informed decisions to help CNCS accomplish its mission.

CNCS also stated that the likelihood and impact analysis were conducted to determine risk for the control weaknesses identified from the GSS, eSPAN, and Momentum security control assessments; however, these risk assessment elements were not documented in the risk assessments. Without determining the likelihood and impact of known system control weaknesses, CNCS is unable to accurately determine the severity of the identified risks. This may result in incorrectly prioritizing risks based on criticality, assigning insufficient resources for remediation of the control weaknesses, and not fully understanding risks to the Corporation.

NIST SP 800-39, Revision 1, *Managing Information Security Risk Organization, Mission, and Information System View,* p. 7*,* states: "The purpose of the risk assessment component is to identify: (i) threats to organizations (i.e., operations, assets, or individuals) or threats directed through organizations against other organizations or the Nation; (ii) vulnerabilities internal and external to organizations; (iii) the harm (i.e., consequences/impact) to organizations that may occur given the potential for threats exploiting vulnerabilities; and (iv) the likelihood that harm will occur. The end result is a determination of risk (i.e., the degree of harm and likelihood of harm occurring)."

intra-tier communication among all stakeholders having a shared interest in the mission/business success of the organization."

[16] Likelihood is the probability that potential risk will occur, measured qualitatively such as low, medium or high.

[17] Impact analysis is determining the extent to which a risk event might affect an organization.

External System Risk Assessments

CNCS did not assess information security risks posed to the Corporation through the use of the following external systems managed by service providers:

- Department of Health and Human Services' Payment Management System (grantee drawdown, advance, disbursement)
- General Service Administration, E2 Travel System (employee travel)
- Department of Agriculture, National Finance Center's Payroll System (employee payroll)
- Department of Treasury, Bureau of Public Debt, WebTA System (employee timekeeping)
- CGI Data Center – Momentum Application (agency financial system)
- Bureau of the Fiscal Service – Federal Investments and Borrowings Branch (National Service Trust fund)
- Invoice Processing Platform (IPP), Federal Reserve Bank of Boston (contractor invoice processing and disbursement)

Although the Director of Accounting and Financial Management Services documented review of the Service Organization Control (SOC) Reports for the above external systems, the CISO did not implement a process for the ISSOs to review the SOC Reports to understand and evaluate information security risks associated with the use of external systems. The CISO indicated that OIT planned to perform information security risk assessments for FY 2018 SOC Reports. Without assessing the risks associated with the use of external information systems, CNCS may not be aware of any risks posed to CNCS that are inherent 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).

The FY 2017 FISMA evaluation report included a recommendation for CNCS to 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.[18] CNCS documented and communicated the risk tolerance, and developed an enterprise risk management strategy. However, the risk register was not fully completed as of September 30, 2018.

The FY 2017 FISMA evaluation report also included a recommendation for CNCS to 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.[19] CNCS indicated that it took corrective action and closed the recommendation. However, we noted that CNCS's risk assessments did not address all required NIST elements.

[18] Recommendation 7, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* p 17, (OIG Report No. 18-03, December 18, 2017).

[19] Recommendation 3, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* p 17, (OIG Report No. 18-03, December 18, 2017).

To assist CNCS in continuing to strengthen its risk management program, we recommend CNCS:

> ***Recommendation 4:*** *Develop and document a comprehensive risk register at the mission and business process level. (Modified Repeat) (FY18 – FISMA – NFR 9)*
>
> ***Recommendation 5:*** *Ensure the system risk assessments include all NIST required risk assessment elements, including the missing elements of likelihood and impact analysis. (Modified Repeat) (FY18 – FISMA – NFR 3)*
>
> ***Recommendation 6:*** *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 should include reviews of the Service Organization Control reports or risk assessments performed for external systems to best understand the known information security risks identified by those external systems, and assess and document the risks to CNCS from the use of these systems. (Repeat) (FY18 – FISMA – NFR 7)*

Security Function: Identify Maturity Model Scoring

The calculated maturity level based on the 12 IG FISMA Metrics questions for the Identify function is Defined (Level 2), Not Effective, as depicted in the chart below:

Function	Count	IG FISMA Metric Questions
Ad-Hoc (level 1)	0	NA
Defined (level 2)	6	5, 7, 9, 10, 11, and 12
Consistently Implemented (level 3)	2	1, and 4*
Managed and Measurable (level 4)	4	2, 3, 6, and 8
Optimized (level 5)	0	NA
Calculated Maturity Level: **Defined (Level 2), Not Effective**		

* Question 4 met the highest maturity level in the reporting metrics of “Consistently Implemented”

The *FY 2018 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* states that within the maturity model context, agencies should perform a risk assessment and identify the optimal maturity level that achieves cost-effective security based on their missions and risks faced, risk appetite, and risk tolerance level.

To assist CNCS in reaching an effective rating for the Identify function area, we recommend CNCS:

> ***Recommendation 7:*** *Perform an analysis of the IG FISMA Metrics related to the security function “Identify” and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. (New)*

Security Function: Protect

4. CNCS Must Improve its Configuration Management Controls

FY 18 IG FISMA Metric Area: *Configuration Management*

The establishment and implementation of documented configuration management policies and procedures are 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. It becomes 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:

The Corporation did not fully document and implement standard baseline configurations for all information system platforms. Specifically, we noted that:

- Although the Corporation documented standard baseline configurations for Microsoft Windows servers, it did not document standard baseline configurations for databases, network devices, VMware ESX, and Web browsers. CNCS determined last year that it would not implement the Center for Internet Security (CIS) baselines on its information technology platforms. CNCS also did not develop standard baselines for all platforms other than Microsoft Windows operating systems. The CISO stated that CNCS developed its own platforms based on vendor recommendations.

- Two out of seven sampled Microsoft Windows production servers, with a total of 64 servers, did not have the standard baseline configurations implemented. The two servers were standalone servers that were not centrally managed. These servers on the CNCS network require manual modification of the baselines and do not receive baseline updates from the CNCS Active Directory domain servers. Management did not monitor the servers to ensure the baselines were applied.

- The Momentum application was configured to disable user accounts after 60 days of inactivity which was not in compliance with the CNCS configuration policy requiring information system accounts to be disabled after 30 days of inactivity. A documented risk acceptance regarding deviation from the CNCS configuration policy for inactive accounts expired in October 2017. Management indicated that due to an oversight, the System Owner, Authorizing Official, Acting Chief Information Office and the CISO did not track the risk acceptance expiration to reassess whether an acceptance of risk was still needed, and formally document acceptance of the risk, if required. After we brought this issue to CNCS, it began the process of reissuing the risk acceptance.

- The Momentum session time-out setting was configured to 60 minutes, which is not in compliance with the required 15 minute time-out setting noted in the Momentum System Security Plan. CNCS indicated that the time-out setting noncompliance was due to an oversight.

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.

Without monitoring for compliance with standard baseline configurations, configurations may be intentionally or inadvertently altered from the approved baseline without management's knowledge.

System Change Controls:

The Corporation did not ensure proper testing of system changes. Specifically, 10 out of 11 reviewed GSS changes (CNCS made a total of 99 GSS system changes) did not have test results documented. CNCS confirmed that it did not maintain documentation for the GSS changes that we reviewed.

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 an 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 documenting testing of system changes, CNCS cannot be sure the information system will operate as intended, potentially causing functionality issues for end users.

The FY 2017 FISMA evaluation report included recommendations for CNCS to address configuration management weaknesses; however, management had not yet completed corrective actions.[20]

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

> ***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. (Repeat) (FY18 – FISMA – NFR 10)*

[20] Recommendations 8 and 9, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 19, (OIG Report No. 18-03, December 18, 2017).

Recommendation 9: *Implement a process to track formal documented risk acceptance forms to reassess whether an acceptance of risk is still needed, and formally document acceptance of the risk, if required prior to the expiration date of current risk acceptance forms. (New) (FY18 – FISMA – NFR 10)*

Recommendation 10: *Implement a process to ensure that functional testing occurred and documentation is maintained for system changes. (Modified Repeat) (FY18 – FISMA – NFR 10)*

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

FY 18 IG FISMA Metric Area: *Identity and Access Management*

Multifactor authentication requires two or more credentials when logging on to information systems. Credentials include something an individual knows, such as a password, and something an individual possess, such as a Personal Identification Verification (PIV) card or fingerprint.

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

CNCS indicated that the PIV project team selected a small pilot group of certain privileged users, and identified network devices and software that needed to be upgraded to support PIV implementation. However, the pilot project was not completed and CNCS did not perform further work on PIV implementation. The CISO stated that the PIV implementation was put on hold due to higher priority operational issues and lack of available resources. At the beginning of the calendar year 2018, CNCS had a major network latency issue that took about four months to resolve. In addition, as Microsoft Windows 10 workstations were being incrementally deployed to the CNCS enterprise, PIV authentication for non-privileged users is planned to be implemented at that time. The available funding for purchasing new computers as part of CNCS regular technology refresh will determine the PIV implementation schedule. Based on current funding levels, the estimated date of completion is at the end of the calendar year 2019.

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.

Furthermore, OMB M-16-04, *Cybersecurity Strategy and Implementation Plan (CSIP) for the Federal Civilian Government*, (Oct. 30, 2016) required federal agencies to have 100 percent of privileged users and 85 percent of non-privileged users authenticate through PIV credentials within Fiscal Year 2016.

Without strong multifactor authentication for local and network access for privileged user accounts, there is an increased risk of unauthorized access 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 any data stored on the network. As a result, the Corporation may be exposed to inappropriate or unauthorized access to sensitive information, including (PII, which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII. In addition, without strong multifactor authentication for network access for non-privileged user accounts, there is increased risk of unauthorized access to CNCS information and information systems by an unauthorized user decreasing the confidentiality and integrity of data.

The FY 2017 FISMA evaluation report included recommendations for CNCS to implement PIV multifactor authentication for privileged and non-privileged users.[21] Due to CNCS's lack of progress in multifactor authentication, all prior year's recommendations remained open.

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

> ***Recommendation 11****: Implement* Personal Identification Verification *multifactor authentication for local and network access for privileged users. (Repeat) (FY18 – FISMA – NFR 4)*
>
> ***Recommendation 12****: Implement* Personal Identification Verification *multifactor authentication for network access for non-privileged users. (Repeat) (FY18 – FISMA – NFR 4)*

6. CNCS Must Strengthen Account Management Controls

FY 18 IG FISMA Metric Area: *Identity and Access Management*

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

Although the network accounts were disabled for three separated employees out of a total population of 178, their accounts were not removed from the Active Directory (AD) Subversion Organizational Unit (OU).[22] Access to the Subversion repository is managed through AD.[23] Therefore, if the AD accounts were re-enabled, the AD accounts would be able to access the Subversion repository increasing the risk of unauthorized modifications to code.

[21] Recommendations 14 and 15, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service***,** p. 23, (OIG Report No. 18-03, December 18, 2017).

[22] An OU is a subdivision in Active Directory to hold users, groups, and computers with designated Group Policy settings and account permissions.

[23] Subversion is the code repository for CNCS software versioning and revision control tool used by CNCS employees and contractor software developers to maintain application source code and documentation.

CNCS stated that access to the Subversion repository is managed via AD and therefore by disabling the AD accounts, access to Subversion is prevented. However, the disabled AD accounts were not removed from the Subversion OU. After we presented the issue to CNCS, CNCS indicated that it would perform account management reviews and clean-up of the Subversion repository OU.

If the separated individual's disabled network accounts are not removed from the AD Subversion OU, and the AD accounts are purposefully or inadvertently re-enabled, the accounts would be able to access Subversion. This presents a risk because Subversion is used to perform review of code in the development environment before it is migrated to the production environment. Inappropriate access to Subversion increases the risk that unauthorized individuals may make unauthorized modifications to code within the development environment and migrate the code into the production environment. Consequently, the unauthorized changes may have adverse effects to the functionality and security of the application.

The FY 2017 FISMA evaluation report included recommendations to disable system accounts for separated individuals.[24] CNCS indicated that corrective action had been taken and considered the recommendations as closed. However, our evaluation determined that the Corporation continued to have control weaknesses related to separated users.

To assist CNCS in continuing to strengthen account management controls, we recommend CNCS:

> ***Recommendation 13:*** *Ensure disabled network accounts for separated individuals are removed from the Active Directory Subversion Organizational Unit. (New) (FY18 – FISMA – NFR 11)*
>
> ***Recommendation 14:*** *Ensure that periodic reviews are conducted of user accounts with access to the Subversion OU within Active Directory. (New) (FY18 – FISMA – NFR 11)*

7. CNCS Must Enhance the Personnel Screening Process

FY 18 IG FISMA Metric Area: *Identity and Access Management*

The purpose of performing background checks is to ascertain the suitability of an individual for a specific position. The depth of background checks should be conducted at the extent and level appropriate to the risks associated with the position and the Corporation. Therefore, the Corporation must consider a risk designation based on sensitivity level of the position when it screens its employees and contractors.

[24] Recommendation 12, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 22, (OIG Report No. 18-03, December 18, 2017).

CNCS did not ensure employees had the proper background investigations. Specifically, 11 employees from a sample of 23 employees and nine contractors with access to the CNCS network and eSPAN had background investigations at a lower level than the risk associated with their assigned positions as noted in their Position Designation Record (PDR).[25] These individuals only had Tier 1 investigations performed, even though their positions required Tier 2 or Tier 4 level investigations based on their PDRs.[26]

Additionally, the investigation levels of the three Momentum privileged users identified in the FY 2017 FISMA evaluation were still below the level commensurate with the risk associated with their assigned positions.[27] These individuals had a National Agency Check with Inquiries (NACI) investigation or Tier 1. These privileged users were CNCS employees with sensitive roles and had permissions in the critical Momentum application that require a higher level of background investigation. Momentum privileged users have the ability to add, modify and delete their own and other users' roles and permissions in the system.

CNCS indicated that due to the loss of eight Office of Human Capital staff with limited funding designated for background investigations, the initiation of new background investigations are being completed on an office-by-office basis, beginning with individuals from the Office of Personnel Security. CNCS stated that currently, eight out of 19 CNCS offices completed background investigations for their employees. In addition, CNCS had not yet developed a schedule to complete background investigations for the remaining employees based on the risk of positions and their sensitivity levels. Based on current staffing and funding level, CNCS estimates completion of all required employee background investigations in the next two years.

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. This can ultimately affect the confidentiality of CNCS data.

The FY 2017 FISMA evaluation report included recommendations for CNCS to perform background investigations at a level commensurate with the risk associated with an individual's assigned positions.[28] CNCS indicated that PDRs were revised using the PDAT tool by the end of 2017 and began the process of initiating new background investigations based on the revised PDRs. Although the investigations are not yet completed, CNCS implemented a process to conduct the background investigations at a level commensurate with the risk designations documented in the PDRs. Therefore, CNCS completed the prior year recommendations and we make new recommendations to address the current weaknesses in background investigations.

[25] The PDRs were based off of the OPM's Position Designation Automated Tool (PDAT).

[26] Tier 1 is an investigation for positions designated as low-risk, non-sensitive (formerly National Agency Check with Inquires). Tier 2 is Moderate risk (formerly Moderate Risk Background Investigation) and Tier 4 is high risk (formerly Background Investigation).

[27] Finding 6, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 18-03, December 18, 2017).

[28] Recommendations 18 and 19, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 18-03, December 18, 2017).

To assist CNCS in continuing to strengthen the personnel screening process, we recommend the CNCS:

> ***Recommendation 15:*** *Perform and document an assessment of staffing and funding levels required for background investigations and address any recognized gaps. (New) (FY18 – FISMA – NFR 2)*
>
> ***Recommendation 16:*** *Develop, document and implement a schedule to prioritize background investigations for individuals with higher level risk as noted in the Position Designation Records. (New) (FY18 – FISMA – NFR 2)*

8. CNCS Must Improve Physical Access Controls

FY 18 IG FISMA 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.

We noted the following issues regarding physical access controls at the Vinton, Iowa NCCC campus, FFMC and Pennsylvania State Office:

- The primary entrance to the FFMC and Philadelphia State Office is a glass door which could pose a security risk to the premises. The design of the shared workspace for FFMC and Philadelphia State Office allows for visitor visibility; however, the FFMC and Philadelphia State Office do not have regular visitors and had not replaced the primary entrance glass door. In addition, an emergency exit door of the FFMC and Philadelphia State Office was left ajar without any sensors notifying CNCS staff that the door was open. The emergency exit door did not have an effective means of ensuring the door shuts completely and securely. Further, alarm sensors were not present on the door to detect potential ingress or intrusion. This was an oversight of the design and security practices at the FFMC and Philadelphia State Office.

- There were neither operated cameras nor CNCS personnel to monitor the FFMC and Philadelphia State Office entry points and key locations. The FFMC and Philadelphia State Office did not maintain or operate any security cameras for its premises, where they are located in a commercial building and the general public can freely access in and out from the building entry/exit points and between building floors. CNCS planned but had yet to purchase cameras for the office space.

- Although cameras were in place at the Vinton NCCC campus, there was no campus personnel monitoring the cameras on a routine basis. The Vinton NCCC staff configured its camera system to be monitored on an as-needed basis via Internet connections; however, the campus did not designate any staff or security personnel to monitor the camera feeds.

- CNCS did not perform a physical security risk assessment for the Vinton NCCC campus. Vinton NCCC campus staff was unaware of the Department of Homeland Security Federal Protective Services (FPS) physical security risk assessment as an available option to assess its facility’s security risk and concerns.

- Although FFMC completed a FPS physical security risk assessment questionnaire, we were unable to validate a risk assessment report was issued by FPS based upon the CNCS questionnaire.

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.

Additionally, *The Risk Management Process for Federal Facilities: An Interagency Security Committee Standard* (Standard), states the following regarding facility risk assessments: "This ISC Standard defines the criteria and processes that those responsible for the security of a facility should use to determine its facility security level, and provides an integrated, single source of physical security countermeasures.[29] The Standard also provides guidance for customization of the countermeasures for Federal facilities."

Standard Section 5.1.2 Identify and Assess Risks, states: "The risks to a facility must first be identified and assessed in order to determine if the baseline LOP [level of protection] is sufficient or if customization is required. [omitted] The facility's security organization will conduct a risk assessment to identify risk(s). When a facility does not have an assigned security organization or Federal tenant with a law enforcement or security element housed in the facility, the FSC shall select a Federal department or agency to provide the services of the security organization."[30]

The lack of adequate controlled access via facility doors to the FFMC and Philadelphia State Office increases the risk of unauthorized access leading to theft, modification or disclosure of sensitive information. In addition, the FFMC and Philadelphia State Office would not have video recordings for review in an event of investigations of unauthorized entry to the facility. Further, there may be a delayed response to incidents of unauthorized entry to the facility as the Vinton NCCC campus does not review video records in real time.

Without a physical security risk assessment, the FFMC, Philadelphia State Office and Vinton NCCC campus may not be aware of threats that could cause serious loss or damage to the facilities, equipment, personnel, and sensitive information.

To assist CNCS in strengthening physical access controls, we recommend CNCS:

> ***Recommendation 17:*** *Require FFMC to implement corrective actions to secure the facility with doors that do not pose a security risk to the facility. (New) (FY18 – FISMA – NFR 5)*
>
> ***Recommendation 18:*** *Require FFMC to implement corrective actions to ensure video recordings of the main entry and key locations within the facility are captured and a process is implemented to monitor the camera feeds. (New) (FY18 – FISMA – NFR 5)*

[29] https://www.dhs.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf; page iii.
[30] https://www.dhs.gov/sites/default/files/publications/isc-risk-management-process-2016-508.pdf; pages 22 – 23.

Recommendation 19: *Require Vinton NCCC campus to implement corrective actions to ensure the camera feeds are monitored. (New) (FY18 – FISMA – NFR 5)*

Recommendation 20: *Require FFMC and the Vinton NCCC campus to conduct and document a physical security risk assessment. (New) (FY18 – FISMA – NFR 5)*

Security Function: Protect Maturity Model Scoring

The calculated maturity level based on the 28 IG FISMA Metric questions for the Protect function is Defined (Level 2), Not Effective, as depicted in the chart below:

Function	Count	IG FISMA Metric Questions
Ad-Hoc (level 1)	6	16, 17,18, 28, 34, and 37
Defined (level 2)	8	15, 19, 21, 23, 24, 26, 29, and 30
Consistently Implemented (level 3)	7	14*, 20*, 25, 33, 35, 36, and 39*
Managed and Measurable (level 4)	5	31, 41, 42, 43, and 44
Optimized (level 5)	2	27 and 40
Calculated Maturity Level: **Defined (Level 2), Not Effective**		

* Question 14, 20, and 39 met the highest maturity level in the reporting metrics of “Consistently Implemented”

To assist CNCS reach an effective rating for the Protect function area, we recommend the CNCS:

Recommendation 21: *Perform an analysis of the IG FISMA Metrics related to the security function “Protect” and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)*

Security Function: Detect

9. CNCS Must Enhance the Review and Analysis of Momentum Audit Logs

FY 18 IG FISMA Metric Area: *Information Security Continuous Monitoring*

An audit log is a document that records a security event, determined by an organization, for an information system. Audit logs act as a detective control because their trails provide evidence of user activity (user logging in, number failed attempt logon, password reset, etc.).

Although the Momentum Oracle logs are collected and monitored by the information system contractor, CNCS did not capture the Momentum Oracle security logs into its security event management system, Splunk, which is an event correlation tool used for continuous audit log review, analysis and reporting.[31] [32] The continuous event and trend analysis to investigate security events are required by NIST for information systems categorized as moderate.[33]

CNCS indicated that due to technical issues with the data center used by the Momentum contractor, the logs from Momentum were not ingested into the CNCS security event management system. In addition, CNCS stated that ingesting logs from Momentum to the Splunk tool became a lower priority due to unresolved issues resulting from a Momentum upgrade that began in August 2017. CNCS is continuing to work with the contractor to correct these ongoing 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 address a prior year FISMA evaluation recommendation,[34] CNCS implemented policies and procedures for the review, analysis and reporting of the Momentum Oracle security logs; however, the process for aggregating the security logs into the security event management system was not completed.

[31] 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.

[32] 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.

[33] FIPS 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.

[34] Recommendations 16 and 17, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service,* p. 24, (OIG Report No. 18-03, December 18, 2017).

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

> ***Recommendation 22****: Complete the process for aggregating the Momentum Oracle database security logs into the security event management system (i.e., Splunk tool). (Repeat) (FY18 – FISMA – NFR 8)*

Security Function: Detect Maturity Model Scoring

The calculated maturity level based on the five IG FISMA Metric questions for the Detect function is Defined (Level 2), Not Effective, as depicted in the chart below:

Function	Count	IG FISMA Metric Questions
Ad-Hoc (level 1)	2	46 and 50
Defined (level 2)	2	48 and 49
Consistently Implemented (level 3)	0	N/A
Managed and Measurable (level 4)	1	47
Optimized (level 5)	0	N/A
Calculated Maturity Level: **Defined (Level 2), Not Effective**		

To assist CNCS reach an effective rating for the Detect function area, we recommend CNCS:

> ***Recommendation 23:*** *Perform an analysis of the IG FISMA Metrics related to the security function "Detect" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)*

Security Function: Respond Maturity Model Scoring

The calculated maturity level based on the seven IG FISMA Metric questions for the Respond function is Consistently Implemented (Level 3), Not Effective, as depicted in the chart below:

Function	Count	IG FISMA Metric Questions
Ad-Hoc (level 1)	0	N/A
Defined (level 2)	0	N/A
Consistently Implemented (level 3)	6	52, 53, 54, 55, 56, and 58
Managed and Measurable (level 4)	1	57*
Optimized (level 5)	0	N/A
Calculated Maturity Level: Consistently Implemented (Level 3), Not Effective		

* Question 57 met the highest maturity level in the reporting metrics of "Managed and Measurable"

To assist CNCS reach an effective rating for the Respond function area, we recommend the CNCS:

> ***Recommendation 24:*** *Perform an analysis of the IG FISMA Metrics related to the security function "Respond" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)*

Security Function: Recover Maturity Model Scoring

The calculated maturity level based on the seven IG FISMA Metric questions for the Recover function is Consistently Implemented (Level 3), Not Effective, as depicted in the chart below.

Function	Count	IG FISMA Metric Questions
Ad-Hoc (level 1)	0	N/A
Defined (level 2)	3	61, 64, and 66
Consistently Implemented (level 3)	4	60*, 62*, 63, and 65*
Managed and Measurable (level 4)	0	N/A
Optimized (level 5)	0	N/A
Calculated Maturity Level: Consistently Implemented (Level 3), Not Effective		

* Question 60, 62, and 65 met the highest maturity level in the reporting metrics of "Consistently Implemented"

To assist CNCS reach an effective rating for the Recover function area, we recommend the CNCS:

Recommendation 25: *Perform an analysis of the IG FISMA Metrics related to the security function "Recover" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (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.[35] 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 (FFMC, NCCC and State Offices). The enterprise level assessment was conducted at the CNCS Headquarters in Washington, D.C., from May 21, 2018 to September 30, 2018. The facility level assessment included on-site security assessments at the Philadelphia, Pennsylvania FFMC and State Office from June 13 to 14, 2018, and Vinton, Iowa NCCC campus from June 28 to 29, 2018 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 Washington, D.C. Headquarters, the Philadelphia FFMC and State Office, and Vinton NCCC campus.

[35] https://www.ignet.gov/sites/default/files/files/committees/inspect-eval/iestds12r.pdf

The evaluation also included a follow up on prior year FISMA evaluation recommendations to determine if CNCS made progress in implementing the recommended improvements concerning its information security program.[36]

Methodology

Following the framework for minimum security controls in NIST SP 800-53, Revision 4, certain controls were selected from NIST security control families associated with FY 2018 IG FISMA Metric Domains aligned with the Cybersecurity Framework Security Functions.[37] For this evaluation, **Table 5** lists the following selected controls for the four CNCS systems that were reviewed:

Table 5: List of Selected Controls Reviewed

Security Control Family	Associated Control[38]
Access Control	AC-1, AC-2, AC-8, and AC-17
Awareness And Training	AT-1, AT-2, AT-3, and AT-4
Security Assessment And Authorization	CA-1, CA-2, CA-3, CA-5, CA-6, CA-7, and CA-8,
Configuration Management	CM-1, CM-2, CM-3, CM-6, CM-7, CM-8, CM-9, and CM-10
Contingency Planning	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, and CP-9
Identification And Authentication	IA-1
Incident Response	IR-1, IR-4 and IR-6
Planning	PL-2, PL-4, and PL-8
Program Management	PM-5, PM-7, PM-8, PM-9 and PM-11
Personnel Security	PS-1, PS-2, PS- 3, and PS-6
Risk Assessment	RA-1, RA-2, and RA-5
System And Services Acquisition	SA-4, SA-3, and SA-8
System And Information Integrity	SI-2, and SI-4
Privacy	AR-1, AR-2, AR-3, AR-4, AR-5, DM-1, SE-1, SE-2, and TR-2

To accomplish the evaluation 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.

[36] *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 18-03, December 18, 2017).

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

[38] These associated controls are from NIST 880-53 Revision 4, https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- Performed site visits to determine if controls are consistently implemented across the Corporation at facility level.
- Reviewed the status of recommendations in the FY 2017 FISMA report, including supporting documentation to ascertain whether the actions taken addressed the weakness.[39]

In selecting and testing for the adequacy and 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. Relative risk, and the significance or criticality of the specific items in achieving the related control objectives was considered. In addition, 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 was considered. In some cases, this resulted in selecting the entire population. However, in cases where the entire audit population was not selected, the results cannot be projected and if projected may be misleading.

[39] Ibid. footnote 39.

STATUS OF PRIOR YEAR RECOMMENDATIONS

Tables 6, 7, 8 and 9 summarize the status of our follow up related to the standing of prior year recommendations reported for the FY 2014, 2015, 2016, and 2017 FISMA evaluations.[40] [41] [42] [43]

From the FY 2014, 2015, 2016, and 2017 FISMA evaluations, the Corporation implemented corrective actions to fully close 24 prior year recommendations. In addition, the Corporation partially closed one prior year recommendation.

Table 6: Status of Prior Year FY 2014 Recommendations

FISMA NFRs	FY 2014 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY14 – 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. *(Modified Repeat, refer to FY17-FISMA-NFR 1)*	Closed	Agree
	Recommendation 5: Perform authenticated vulnerability scans weekly of the critical Corporation applications and databases (eSPAN, eGrants, MyAmeriCorps portal). *(Modified Repeat, refer to FY17-FISMA-NFR 1)*	Closed	Agree
FY14 – FISMA – NFR 9	**Recommendation 1:** Document and fully implement a comprehensive and enterprise-wide risk management process, including the following:		

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

[41] *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).

[42] *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).

[43] Ibid. footnote 39.

FISMA NFRs	FY 2014 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	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 *(Modified Repeat, refer to FY17-FISMA-NFR 8)*	Closed	Agree
	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. *(Modified Repeat, refer to FY17-FISMA-NFR 8)*	Closed	Disagree Modified Repeat, refer to Finding 3
	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. *(Modified Repeat, refer to FY17-FISMA-NFR 8)*	Closed	Disagree Modified Repeat, refer to Finding 3
FY14 – FISMA – NFR 10	**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. *(Modified Repeat, refer to FY17-FISMA-NFR 2)*	Closed	Agree
	Part D: SSPs accurately describe the implementation details for the base NIST SP 800-53 security and privacy controls and required control enhancements. *(Modified Repeat, refer to FY17-FISMA-NFR 2)*	Closed	Agree

FISMA NFRs	FY 2014 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY14 – FISMA – NFR 14	**Recommendation 1:** Develop a more effective and comprehensive DRP and COOP by:		
	Part E: Updating the COOP based on revisions to the BIA and DRP. *(Modified Repeat, refer to FY17-FISMA-NFR 4)*	Closed	Agree

Table 7: Status of Prior Year FY 2015 Recommendations

FISMA NFRs	FY 2015 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY15 – 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. *(Modified Repeat, refer to FY17-FISMA-NFR 10)*	Closed	Agree
FY15 – 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. *(Modified Repeat, refer to FY17-FISMA-NFR 1)*	Closed	Agree

Table 8: Status of Prior Year FY 2016 Recommendations

FISMA NFRs	FY 2016 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY16 – FISMA – NFR 1	**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 4

FISMA NFRs	FY 2016 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	(Modified Repeat, refer to FY17-FISMA-NFR 5)		
	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. *(Modified Repeat, refer to FY17-FISMA-NFR 5)*	Open	Agree Modified Repeat, refer to Finding 4
	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. *(Modified Repeat, refer to FY17-FISMA-NFR 5)*	Open	Agree Modified Repeat, refer to Finding 4
FY16 – FISMA – NFR 2	**Recommendation 3:** Develop a service level agreement (SLA) or performance metrics to ensure that GSS backups are performed in accordance with contractual requirements. *(Modified Repeat, refer to FY17-FISMA-NFR 4)*	Closed	Agree

Table 9: Status of Prior Year FY 2017 Recommendations

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY17-FISMA-NFR 2	**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.	Closed	Agree
	Recommendation 2: Ensure the control implementation descriptions for the privacy controls are documented in the GSS, eSPAN and Momentum system security plans.	Closed	Agree
	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.	Closed	Disagree Modified Repeat, refer to Finding 3
	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	Open	Agree Modified Repeat, refer to Finding 3

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	gain an understanding of the information security risks identified, and assess and document the risks to CNCS from the use of these systems.		
FY17-FISMA-NFR 3	**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.	Closed	Agree
	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.	Closed	Agree
FY17-FISMA-NFR 8	**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	Closed	Disagree Modified Repeat, refer to Finding 3

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	evaluating risk across the organization with respect to the organization's risk tolerance • Developing, documenting, and implementing approaches for monitoring risk over time		
FY17-FISMA-NFR 5	**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.	Open	Agree Modified Repeat, refer to Finding 4
	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.	Open	Agree Modified Repeat, refer to Finding 4
FY17-FISMA-NFR 10	**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.	Closed	Agree
	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.	Closed	Agree

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	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.	Closed	Agree
	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.	Closed	Agree
FY17-FISMA-NFR 9	**Recommendation 14**: Implement PIV multifactor authentication for local and network access for privileged users.	Open	Agree Repeat, refer to Finding 5
	Recommendation 15: Implement PIV multifactor authentication for network access for non-privileged users.	Open	Agree Repeat, refer to Finding 5
FY17-FISMA-NFR 7	**Recommendation 16**: Complete the process for aggregating the Momentum Oracle	Open	Agree

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	database security logs into the Splunk tool.		Repeat, refer to Finding 9
	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.	Closed	Agree
FY17-FISMA-NFR 6	**Recommendation 18:** Complete the updates to the role designation chart specifying the type of background investigation required by position and sensitivity levels.	Closed	Agree
	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.	Closed	Agree
FY17-FISMA-NFR 4	**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.	Open	Agree The disaster recovery test was scheduled in September and an after action report was not available during the fieldwork period for us to review.
	Recommendation 21: Update the COOP based on revisions to the BIA and DRP.	Closed	Agree
	Recommendation 22: Develop and implement a SLA or performance metrics to ensure that GSS backups are performed in accordance with contractual requirements.	Closed	Agree
FY17-FISMA-NFR 1	**Recommendation 23:** Enforce the agency-wide information security program across the	Closed	Agree

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	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.		
	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.	Open	Agree Modified Repeat, refer to Finding 1
	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.	Open	Agree Although this issue was not found for the site visits conducted this year, we did not revisit the CNCS sites from last year where the issues were found to

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
			validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	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	Open	Agree Although this issue was not found for the site visits conducted this year, we did not revisit the CNCS sites from last year where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	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	Open	Agree Although this issue was not found for the site visits conducted this year, we did not revisit the CNCS sites from last year where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	Recommendation 28: Ensure the Vicksburg NCCC campus implements the following regarding the OpenDNS service:	Open	Agree Although this issue was not found for the site visits conducted this

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	- Remove the unnecessary account to the OpenDNS service, and create a new account for administrative access. - Review the OpenDNS reports for the wireless network.		year, we did not revisit the CNCS sites from last year where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	Recommendation 29: Configure CNCS issued laptops to deny the use of the FEMA wireless network by service set identifier (SSID).	Open	Agree Although this issue was not found for the site visits conducted this year, we did not revisit the CNCS sites from last year where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	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.	Open	Agree Although this issue was not found for the site visits conducted this year, we did not revisit the CNCS sites from last year where the issues were found to validate corrective action was completed at those sites. Management stated corrective action was not completed.
	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.	Closed	Agree

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	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.	Closed	Disagree Management's position is that there is no requirement for monitoring video camera feeds. Cameras are implemented for forensic capabilities and are not actively monitored. Per NIST SP 800-53, Revision 4, Control PE-6 Control Enhancement 1, organizations are required to monitor surveillance equipment.
	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.	Closed	Agree
	Recommendation 34: Ensure the Jackson State Office installs a fire extinguisher and smoke detectors.	Closed	Agree

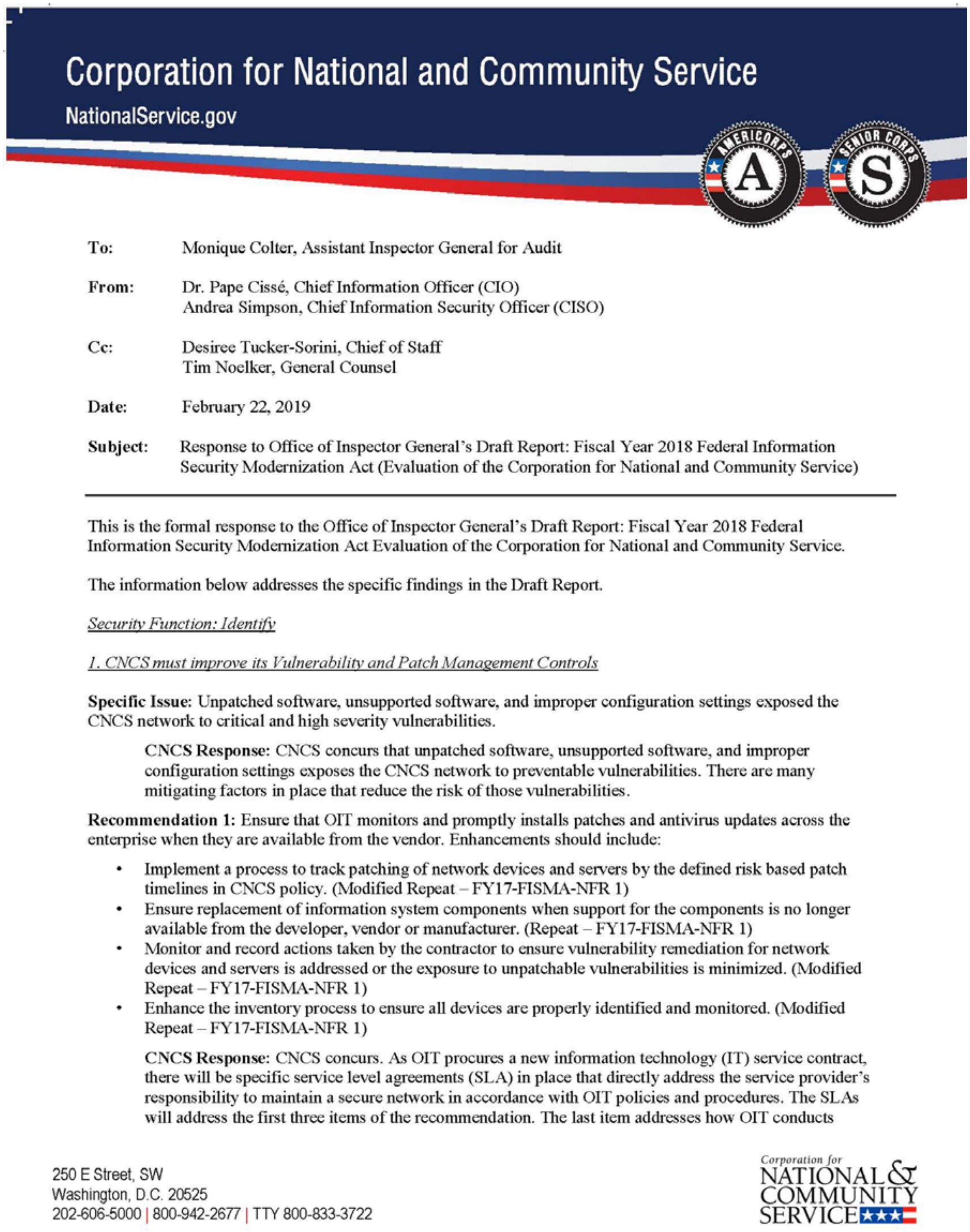
INDEPENDENT ASSESSOR EVALUATION

Table 10 summarizes the results of the independent subjective, judgmental assessment of the agency's information security program.

Table 10: Independent Assessor Evaluation

Security Function	IG FISMA Metric Domains	Independent Assessor Evaluation FY 2018
Identify	Risk Management	Not Effective
Protect	Configuration Management	Not Effective
	Identity and Access Management	Not Effective
	Data Protection and Privacy	Effective
	Security Training	Effective
Detect	Information Security Continuous Monitoring	Not Effective
Respond	Incident Response	Effective
Recover	Contingency Planning	Effective
Overall Assessment: Not Effective		

MANAGEMENT COMMENTS



Corporation for National and Community Service

NationalService.gov

To: Monique Colter, Assistant Inspector General for Audit

From: Dr. Pape Cissé, Chief Information Officer (CIO)
Andrea Simpson, Chief Information Security Officer (CISO)

Cc: Desiree Tucker-Sorini, Chief of Staff
Tim Noelker, General Counsel

Date: February 22, 2019

Subject: Response to Office of Inspector General's Draft Report: Fiscal Year 2018 Federal Information Security Modernization Act (Evaluation of the Corporation for National and Community Service)

This is the formal response to the Office of Inspector General's Draft Report: Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service.

The information below addresses the specific findings in the Draft Report.

Security Function: Identify

1. CNCS must improve its Vulnerability and Patch Management Controls

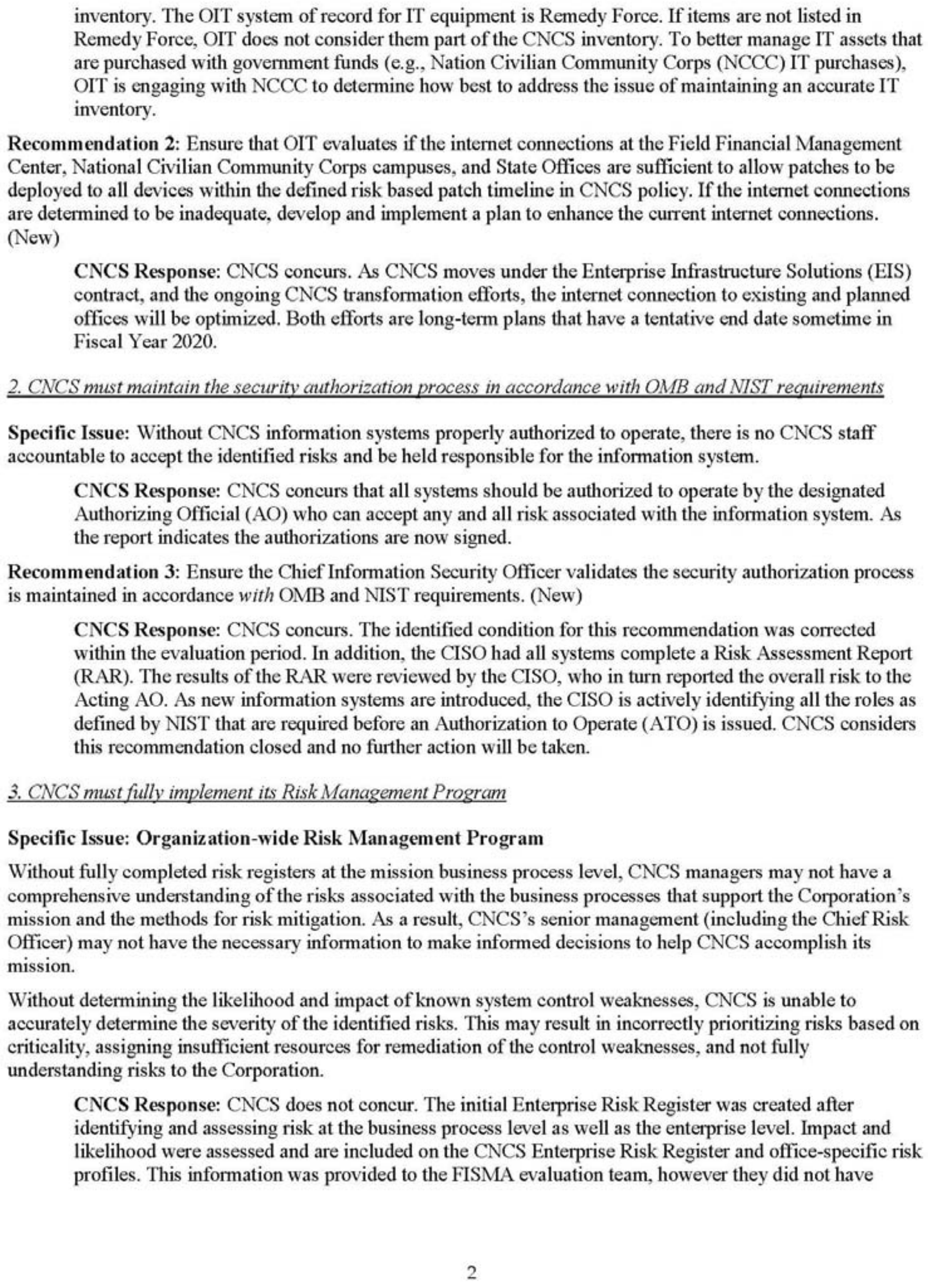
Specific Issue: Unpatched software, unsupported software, and improper configuration settings exposed the CNCS network to critical and high severity vulnerabilities.

> **CNCS Response:** CNCS concurs that unpatched software, unsupported software, and improper configuration settings exposes the CNCS network to preventable vulnerabilities. There are many mitigating factors in place that reduce the risk of those vulnerabilities.

Recommendation 1: Ensure that OIT monitors and promptly installs patches and antivirus updates across the enterprise when they are available from the vendor. Enhancements should include:

- Implement a process to track patching of network devices and servers by the defined risk based patch timelines in CNCS policy. (Modified Repeat – FY17-FISMA-NFR 1)
- Ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer. (Repeat – FY17-FISMA-NFR 1)
- Monitor and record actions taken by the contractor to ensure vulnerability remediation for network devices and servers is addressed or the exposure to unpatchable vulnerabilities is minimized. (Modified Repeat – FY17-FISMA-NFR 1)
- Enhance the inventory process to ensure all devices are properly identified and monitored. (Modified Repeat – FY17-FISMA-NFR 1)

> **CNCS Response:** CNCS concurs. As OIT procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with OIT policies and procedures. The SLAs will address the first three items of the recommendation. The last item addresses how OIT conducts



inventory. The OIT system of record for IT equipment is Remedy Force. If items are not listed in Remedy Force, OIT does not consider them part of the CNCS inventory. To better manage IT assets that are purchased with government funds (e.g., Nation Civilian Community Corps (NCCC) IT purchases), OIT is engaging with NCCC to determine how best to address the issue of maintaining an accurate IT inventory.

Recommendation 2: Ensure that OIT evaluates if the internet connections at the Field Financial Management Center, National Civilian Community Corps campuses, and State Offices are sufficient to allow patches to be deployed to all devices within the defined risk based patch timeline in CNCS policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections. (New)

> **CNCS Response:** CNCS concurs. As CNCS moves under the Enterprise Infrastructure Solutions (EIS) contract, and the ongoing CNCS transformation efforts, the internet connection to existing and planned offices will be optimized. Both efforts are long-term plans that have a tentative end date sometime in Fiscal Year 2020.

2. CNCS must maintain the security authorization process in accordance with OMB and NIST requirements

Specific Issue: Without CNCS information systems properly authorized to operate, there is no CNCS staff accountable to accept the identified risks and be held responsible for the information system.

> **CNCS Response:** CNCS concurs that all systems should be authorized to operate by the designated Authorizing Official (AO) who can accept any and all risk associated with the information system. As the report indicates the authorizations are now signed.

Recommendation 3: Ensure the Chief Information Security Officer validates the security authorization process is maintained in accordance *with* OMB and NIST requirements. (New)

> **CNCS Response:** CNCS concurs. The identified condition for this recommendation was corrected within the evaluation period. In addition, the CISO had all systems complete a Risk Assessment Report (RAR). The results of the RAR were reviewed by the CISO, who in turn reported the overall risk to the Acting AO. As new information systems are introduced, the CISO is actively identifying all the roles as defined by NIST that are required before an Authorization to Operate (ATO) is issued. CNCS considers this recommendation closed and no further action will be taken.

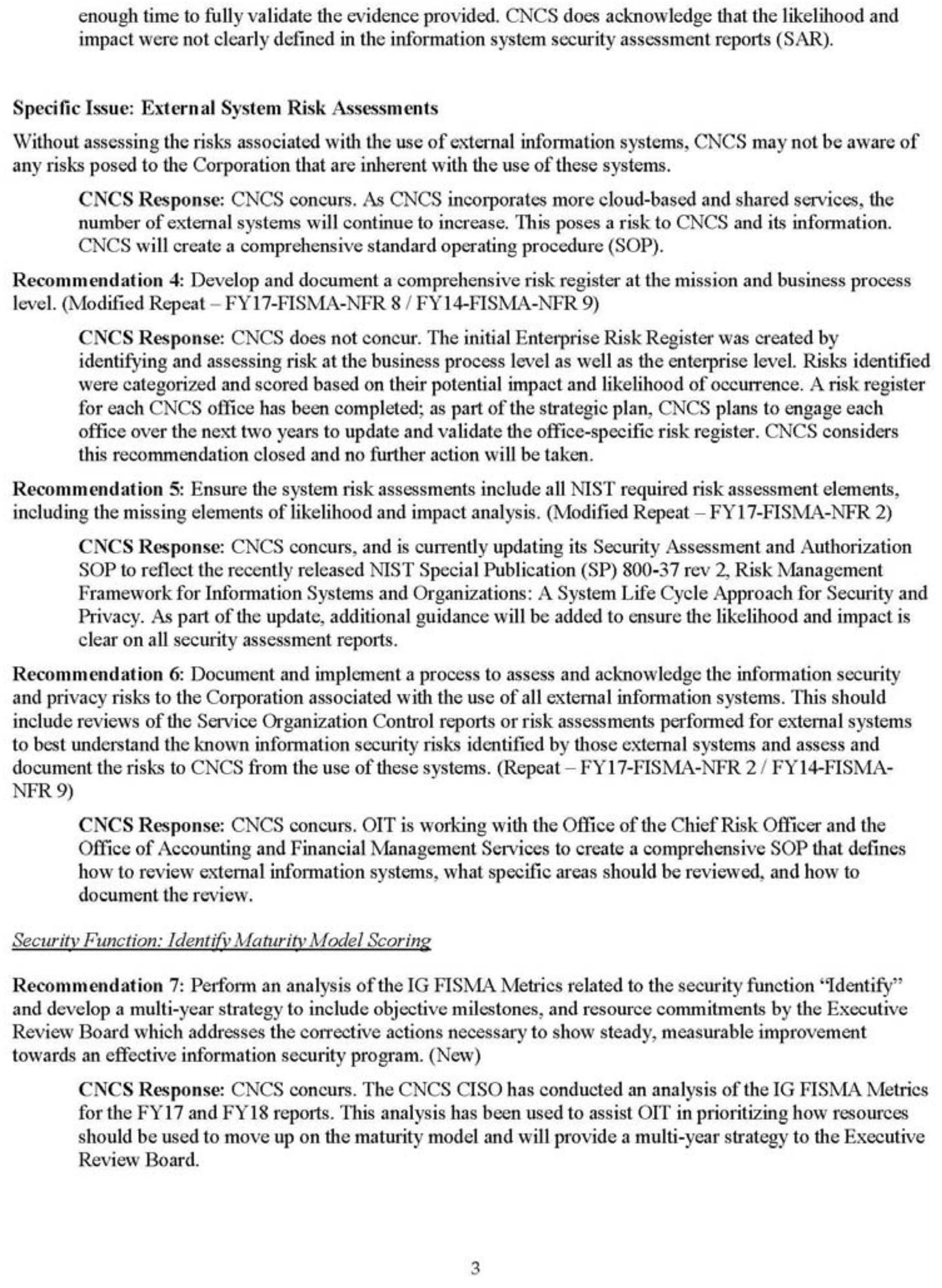
3. CNCS must fully implement its Risk Management Program

Specific Issue: Organization-wide Risk Management Program

Without fully completed risk registers at the mission business process level, CNCS managers may not have a comprehensive understanding of the risks associated with the business processes that support the Corporation's mission and the methods for risk mitigation. As a result, CNCS's senior management (including the Chief Risk Officer) may not have the necessary information to make informed decisions to help CNCS accomplish its mission.

Without determining the likelihood and impact of known system control weaknesses, CNCS is unable to accurately determine the severity of the identified risks. This may result in incorrectly prioritizing risks based on criticality, assigning insufficient resources for remediation of the control weaknesses, and not fully understanding risks to the Corporation.

> **CNCS Response:** CNCS does not concur. The initial Enterprise Risk Register was created after identifying and assessing risk at the business process level as well as the enterprise level. Impact and likelihood were assessed and are included on the CNCS Enterprise Risk Register and office-specific risk profiles. This information was provided to the FISMA evaluation team, however they did not have



enough time to fully validate the evidence provided. CNCS does acknowledge that the likelihood and impact were not clearly defined in the information system security assessment reports (SAR).

Specific Issue: External System Risk Assessments

Without assessing the risks associated with the use of external information systems, CNCS may not be aware of any risks posed to the Corporation that are inherent with the use of these systems.

> **CNCS Response:** CNCS concurs. As CNCS incorporates more cloud-based and shared services, the number of external systems will continue to increase. This poses a risk to CNCS and its information. CNCS will create a comprehensive standard operating procedure (SOP).

Recommendation 4: Develop and document a comprehensive risk register at the mission and business process level. (Modified Repeat – FY17-FISMA-NFR 8 / FY14-FISMA-NFR 9)

> **CNCS Response:** CNCS does not concur. The initial Enterprise Risk Register was created by identifying and assessing risk at the business process level as well as the enterprise level. Risks identified were categorized and scored based on their potential impact and likelihood of occurrence. A risk register for each CNCS office has been completed; as part of the strategic plan, CNCS plans to engage each office over the next two years to update and validate the office-specific risk register. CNCS considers this recommendation closed and no further action will be taken.

Recommendation 5: Ensure the system risk assessments include all NIST required risk assessment elements, including the missing elements of likelihood and impact analysis. (Modified Repeat – FY17-FISMA-NFR 2)

> **CNCS Response:** CNCS concurs, and is currently updating its Security Assessment and Authorization SOP to reflect the recently released NIST Special Publication (SP) 800-37 rev 2, Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy. As part of the update, additional guidance will be added to ensure the likelihood and impact is clear on all security assessment reports.

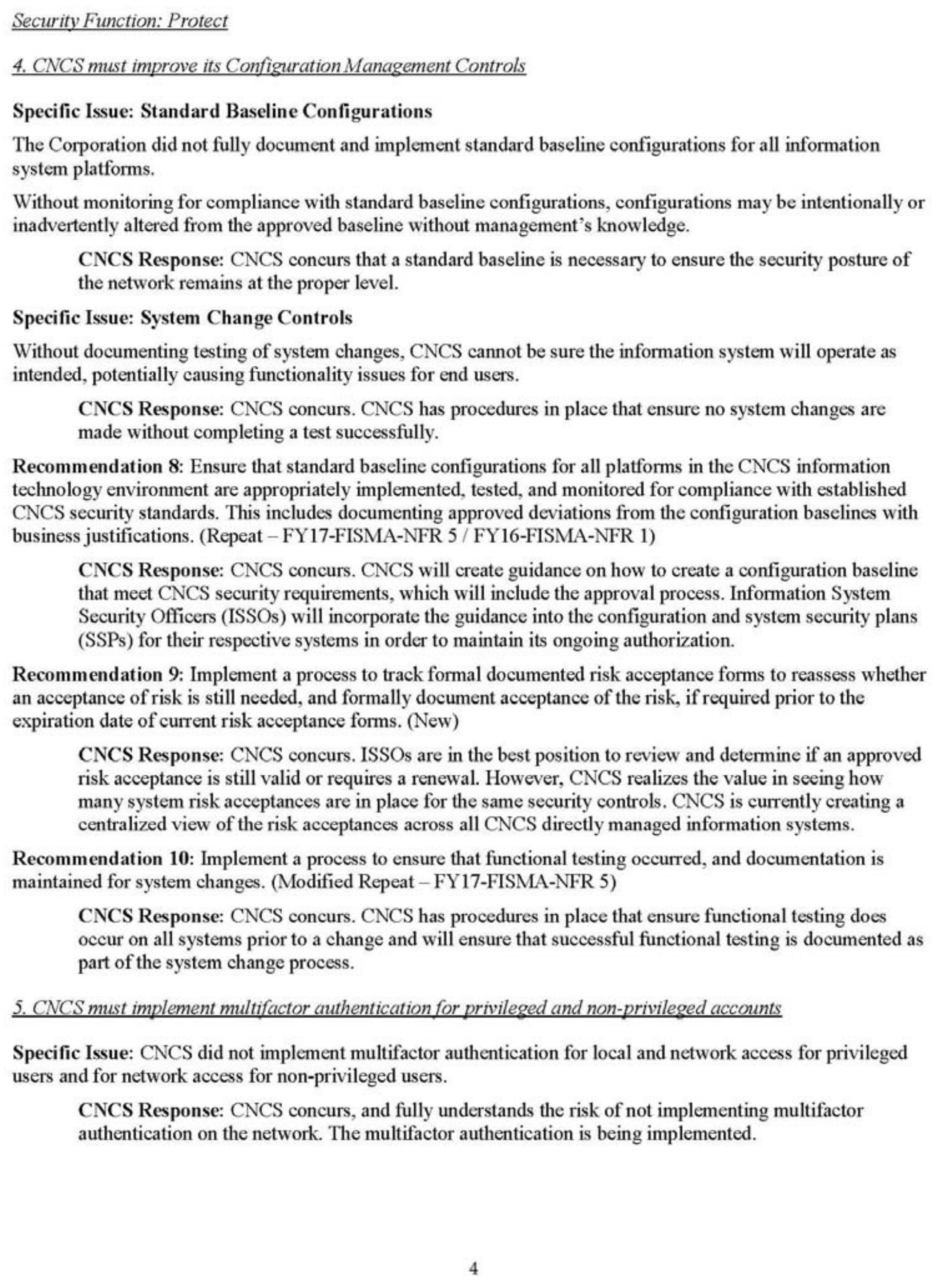
Recommendation 6: Document and implement a process to assess and acknowledge the information security and privacy risks to the Corporation associated with the use of all external information systems. This should include reviews of the Service Organization Control reports or risk assessments performed for external systems to best understand the known information security risks identified by those external systems and assess and document the risks to CNCS from the use of these systems. (Repeat – FY17-FISMA-NFR 2 / FY14-FISMA-NFR 9)

> **CNCS Response:** CNCS concurs. OIT is working with the Office of the Chief Risk Officer and the Office of Accounting and Financial Management Services to create a comprehensive SOP that defines how to review external information systems, what specific areas should be reviewed, and how to document the review.

Security Function: Identify Maturity Model Scoring

Recommendation 7: Perform an analysis of the IG FISMA Metrics related to the security function "Identify" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. (New)

> **CNCS Response:** CNCS concurs. The CNCS CISO has conducted an analysis of the IG FISMA Metrics for the FY17 and FY18 reports. This analysis has been used to assist OIT in prioritizing how resources should be used to move up on the maturity model and will provide a multi-year strategy to the Executive Review Board.



Security Function: Protect

4. CNCS must improve its Configuration Management Controls

Specific Issue: Standard Baseline Configurations

The Corporation did not fully document and implement standard baseline configurations for all information system platforms.

Without monitoring for compliance with standard baseline configurations, configurations may be intentionally or inadvertently altered from the approved baseline without management's knowledge.

> **CNCS Response:** CNCS concurs that a standard baseline is necessary to ensure the security posture of the network remains at the proper level.

Specific Issue: System Change Controls

Without documenting testing of system changes, CNCS cannot be sure the information system will operate as intended, potentially causing functionality issues for end users.

> **CNCS Response:** CNCS concurs. CNCS has procedures in place that ensure no system changes are made without completing a test successfully.

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. (Repeat – FY17-FISMA-NFR 5 / FY16-FISMA-NFR 1)

> **CNCS Response:** CNCS concurs. CNCS will create guidance on how to create a configuration baseline that meet CNCS security requirements, which will include the approval process. Information System Security Officers (ISSOs) will incorporate the guidance into the configuration and system security plans (SSPs) for their respective systems in order to maintain its ongoing authorization.

Recommendation 9: Implement a process to track formal documented risk acceptance forms to reassess whether an acceptance of risk is still needed, and formally document acceptance of the risk, if required prior to the expiration date of current risk acceptance forms. (New)

> **CNCS Response:** CNCS concurs. ISSOs are in the best position to review and determine if an approved risk acceptance is still valid or requires a renewal. However, CNCS realizes the value in seeing how many system risk acceptances are in place for the same security controls. CNCS is currently creating a centralized view of the risk acceptances across all CNCS directly managed information systems.

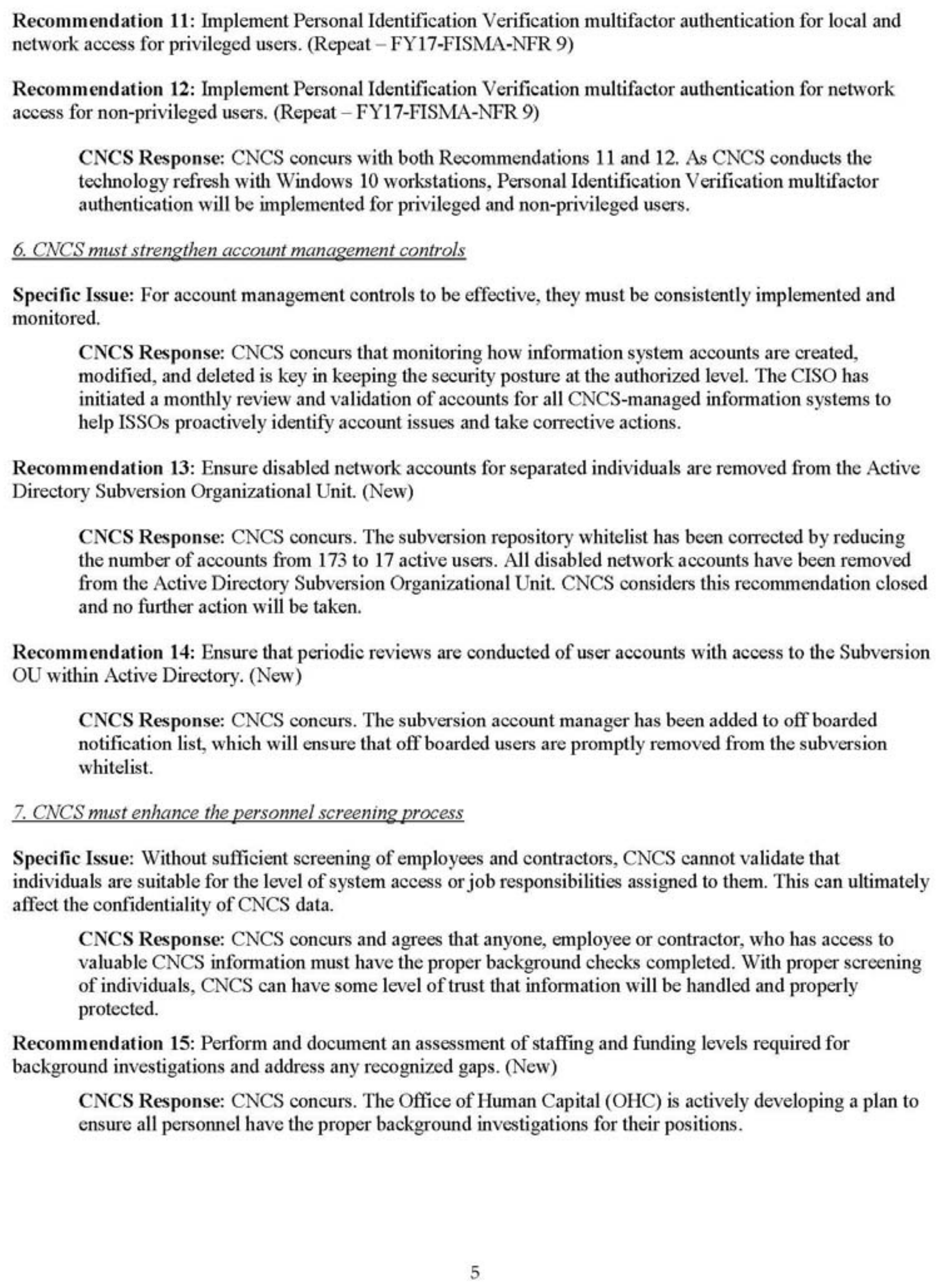
Recommendation 10: Implement a process to ensure that functional testing occurred, and documentation is maintained for system changes. (Modified Repeat – FY17-FISMA-NFR 5)

> **CNCS Response:** CNCS concurs. CNCS has procedures in place that ensure functional testing does occur on all systems prior to a change and will ensure that successful functional testing is documented as part of the system change process.

5. CNCS must implement multifactor authentication for privileged and non-privileged accounts

Specific Issue: CNCS did not implement multifactor authentication for local and network access for privileged users and for network access for non-privileged users.

> **CNCS Response:** CNCS concurs, and fully understands the risk of not implementing multifactor authentication on the network. The multifactor authentication is being implemented.



Recommendation 11: Implement Personal Identification Verification multifactor authentication for local and network access for privileged users. (Repeat – FY17-FISMA-NFR 9)

Recommendation 12: Implement Personal Identification Verification multifactor authentication for network access for non-privileged users. (Repeat – FY17-FISMA-NFR 9)

> **CNCS Response:** CNCS concurs with both Recommendations 11 and 12. As CNCS conducts the technology refresh with Windows 10 workstations, Personal Identification Verification multifactor authentication will be implemented for privileged and non-privileged users.

6. CNCS must strengthen account management controls

Specific Issue: For account management controls to be effective, they must be consistently implemented and monitored.

> **CNCS Response:** CNCS concurs that monitoring how information system accounts are created, modified, and deleted is key in keeping the security posture at the authorized level. The CISO has initiated a monthly review and validation of accounts for all CNCS-managed information systems to help ISSOs proactively identify account issues and take corrective actions.

Recommendation 13: Ensure disabled network accounts for separated individuals are removed from the Active Directory Subversion Organizational Unit. (New)

> **CNCS Response:** CNCS concurs. The subversion repository whitelist has been corrected by reducing the number of accounts from 173 to 17 active users. All disabled network accounts have been removed from the Active Directory Subversion Organizational Unit. CNCS considers this recommendation closed and no further action will be taken.

Recommendation 14: Ensure that periodic reviews are conducted of user accounts with access to the Subversion OU within Active Directory. (New)

> **CNCS Response:** CNCS concurs. The subversion account manager has been added to off boarded notification list, which will ensure that off boarded users are promptly removed from the subversion whitelist.

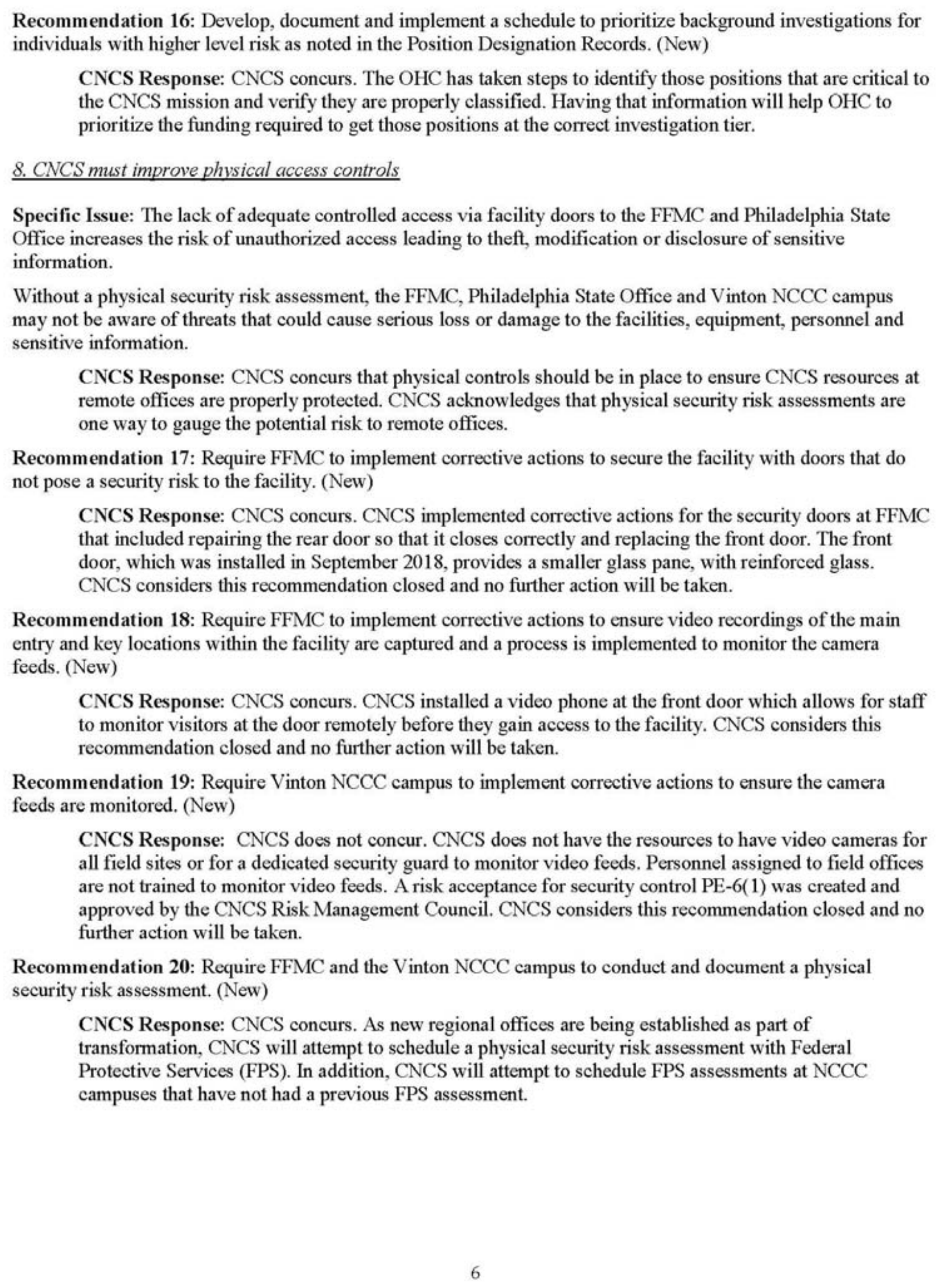
7. CNCS must enhance the personnel screening process

Specific Issue: 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. This can ultimately affect the confidentiality of CNCS data.

> **CNCS Response:** CNCS concurs and agrees that anyone, employee or contractor, who has access to valuable CNCS information must have the proper background checks completed. With proper screening of individuals, CNCS can have some level of trust that information will be handled and properly protected.

Recommendation 15: Perform and document an assessment of staffing and funding levels required for background investigations and address any recognized gaps. (New)

> **CNCS Response:** CNCS concurs. The Office of Human Capital (OHC) is actively developing a plan to ensure all personnel have the proper background investigations for their positions.



Recommendation 16: Develop, document and implement a schedule to prioritize background investigations for individuals with higher level risk as noted in the Position Designation Records. (New)

> **CNCS Response:** CNCS concurs. The OHC has taken steps to identify those positions that are critical to the CNCS mission and verify they are properly classified. Having that information will help OHC to prioritize the funding required to get those positions at the correct investigation tier.

8. CNCS must improve physical access controls

Specific Issue: The lack of adequate controlled access via facility doors to the FFMC and Philadelphia State Office increases the risk of unauthorized access leading to theft, modification or disclosure of sensitive information.

Without a physical security risk assessment, the FFMC, Philadelphia State Office and Vinton NCCC campus may not be aware of threats that could cause serious loss or damage to the facilities, equipment, personnel and sensitive information.

> **CNCS Response:** CNCS concurs that physical controls should be in place to ensure CNCS resources at remote offices are properly protected. CNCS acknowledges that physical security risk assessments are one way to gauge the potential risk to remote offices.

Recommendation 17: Require FFMC to implement corrective actions to secure the facility with doors that do not pose a security risk to the facility. (New)

> **CNCS Response:** CNCS concurs. CNCS implemented corrective actions for the security doors at FFMC that included repairing the rear door so that it closes correctly and replacing the front door. The front door, which was installed in September 2018, provides a smaller glass pane, with reinforced glass. CNCS considers this recommendation closed and no further action will be taken.

Recommendation 18: Require FFMC to implement corrective actions to ensure video recordings of the main entry and key locations within the facility are captured and a process is implemented to monitor the camera feeds. (New)

> **CNCS Response:** CNCS concurs. CNCS installed a video phone at the front door which allows for staff to monitor visitors at the door remotely before they gain access to the facility. CNCS considers this recommendation closed and no further action will be taken.

Recommendation 19: Require Vinton NCCC campus to implement corrective actions to ensure the camera feeds are monitored. (New)

> **CNCS Response:** CNCS does not concur. CNCS does not have the resources to have video cameras for all field sites or for a dedicated security guard to monitor video feeds. Personnel assigned to field offices are not trained to monitor video feeds. A risk acceptance for security control PE-6(1) was created and approved by the CNCS Risk Management Council. CNCS considers this recommendation closed and no further action will be taken.

Recommendation 20: Require FFMC and the Vinton NCCC campus to conduct and document a physical security risk assessment. (New)

> **CNCS Response:** CNCS concurs. As new regional offices are being established as part of transformation, CNCS will attempt to schedule a physical security risk assessment with Federal Protective Services (FPS). In addition, CNCS will attempt to schedule FPS assessments at NCCC campuses that have not had a previous FPS assessment.

Security Function: Protect Maturity Model Scoring

Recommendation 21: Perform an analysis of the IG FISMA Metrics related to the security function "Protect" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)

> **CNCS Response:** CNCS concurs. The CNCS CISO has conducted an analysis of the IG FISMA Metrics for the FY17 and FY18 reports. This analysis has been used to assist OIT in prioritizing how resources should be used to move up on the maturity model and will provide a multi-year strategy to the Executive Review Board.

Security Function: Detect

9. CNCS must enhance the review and analysis of Momentum audit logs

Specific Issue: 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.

> **CNCS Response:** CNCS concurs that having a wide view of all security activities on all systems is important. CNCS relies on the ISSOs to analyze and review the audit events for systems they manage. ISSOs are in the best position to identify any anomalies that may occur within their system.

Recommendation 22: Complete the process for aggregating the Momentum Oracle database security logs into the security event management system (i.e., Splunk tool). (Repeat – FY17-FISMA-NFR 7)

> **CNCS Response:** CNCS concurs. As part of the future direction of Momentum, CNCS will assess what type of information should be ingested into the CNCS SIEM tool. This is not a high priority for CNCS since log reviews are conducted by the Momentum IT support contractor.

Security Function: Detect Maturity Model Scoring

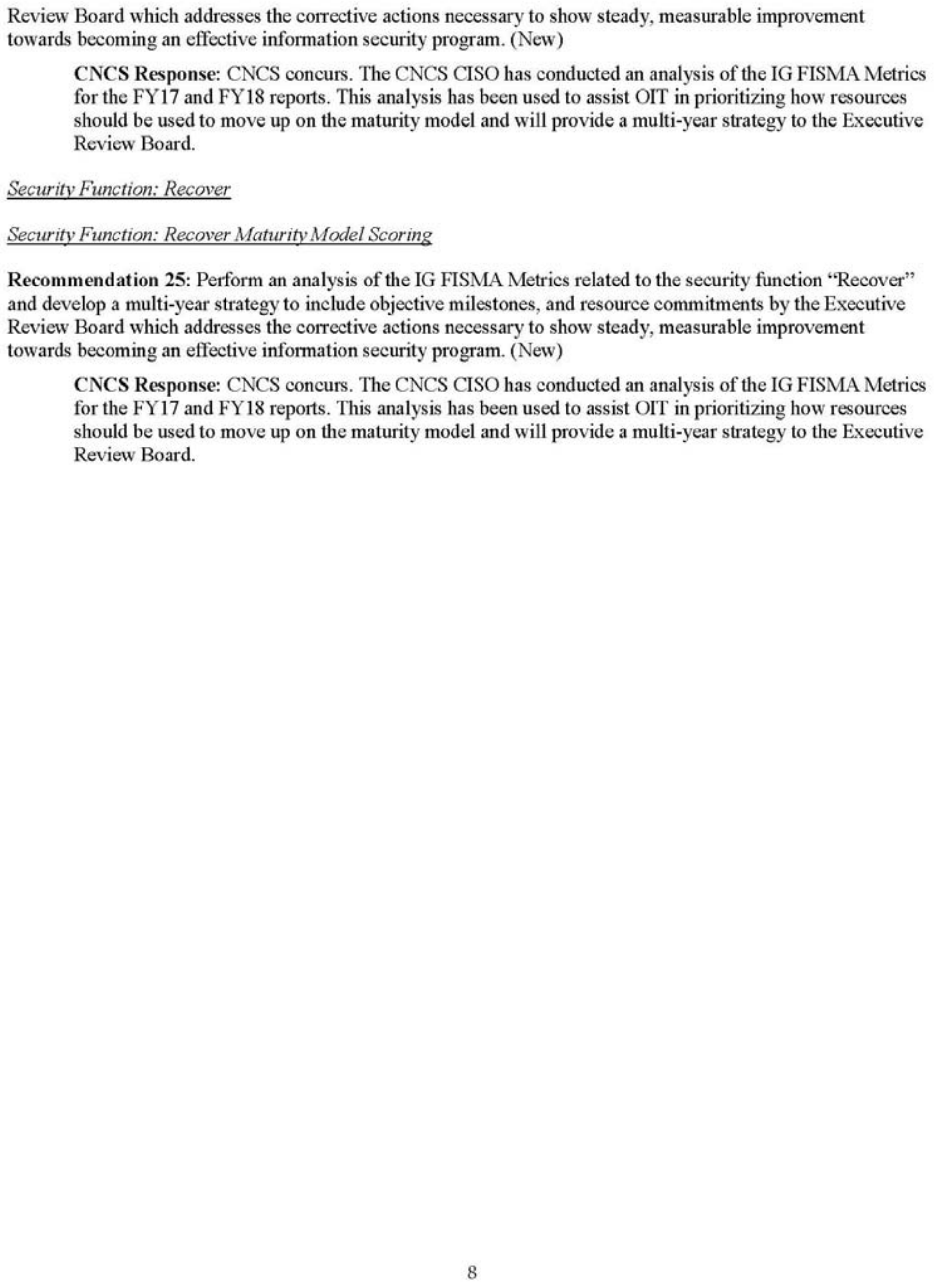
Recommendation 23: Perform an analysis of the IG FISMA Metrics related to the security function "Detect" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)

> **CNCS Response:** CNCS concurs. The CNCS CISO has conducted an analysis of the IG FISMA Metrics for the FY17 and FY18 reports. This analysis has been used to assist OIT in prioritizing how resources should be used to move up on the maturity model and will provide a multi-year strategy to the Executive Review Board.

Security Function: Respond

Security Function: Respond Maturity Model Scoring

Recommendation 24: Perform an analysis of the IG FISMA Metrics related to the security function "Respond" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive



Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)

> **CNCS Response:** CNCS concurs. The CNCS CISO has conducted an analysis of the IG FISMA Metrics for the FY17 and FY18 reports. This analysis has been used to assist OIT in prioritizing how resources should be used to move up on the maturity model and will provide a multi-year strategy to the Executive Review Board.

Security Function: Recover

Security Function: Recover Maturity Model Scoring

Recommendation 25: Perform an analysis of the IG FISMA Metrics related to the security function "Recover" and develop a multi-year strategy to include objective milestones, and resource commitments by the Executive Review Board which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program. (New)

> **CNCS Response:** CNCS concurs. The CNCS CISO has conducted an analysis of the IG FISMA Metrics for the FY17 and FY18 reports. This analysis has been used to assist OIT in prioritizing how resources should be used to move up on the maturity model and will provide a multi-year strategy to the Executive Review Board.

OFFICE OF INSPECTOR GENERAL

CORPORATION FOR

NATIONAL & COMMUNITY SERVICE

CORPORATION FOR NATIONAL & COMMUNITY SERVICE
250 E ST SW, WASHINGTON, DC 20525
202.606.5000 | WWW.NATIONALSERVICE.GOV/

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