

CORPORATION FOR NATIONAL & COMMUNITY SERVICE

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2019 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG Report 20-03

Prepared by:

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



This report was issued to Corporation management on January 24, 2020. 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 July 24, 2020, and complete its corrective actions by January 25, 2021. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.



January 24, 2020

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 2019 Federal Information Security Modernization Act
Evaluation of the Corporation for National and Community Service
(OIG Report 20-03)

Enclosed is the final report on the *Fiscal Year 2019 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service*, the Office of Inspector General's (OIG) Report 20-03. 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 July 24, 2020. Notice of final action is due by January 25, 2021.

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

Enclosure:
As stated

cc: Lisa Guccione, Chief of Staff
Timothy Noelker, General Counsel
Scott Hefter, Chief Operating Officer
Andrea Simpson, Chief Information Security Officer
Jill Graham, Acting Chief Risk Officer
Doug Hilton, Acting Chief Financial Officer
Rachel Turner, Audits and Investigations Program Manager
Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP



**Corporation for National and Community Service
Federal Information Security Modernization Act Evaluation**

Fiscal Year 2019

January 23, 2020

Final Report



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

January 23, 2020

Barbara Stewart, Chief Executive Officer
Corporation for National and Community Service
250 E Street, 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, in accordance with FISMA, Office of Management and Budget (OMB) requirements, and National Institute of Standards and Technology (NIST) guidance. The Corporation for National and Community Service, Office of Inspector General (CNCS-OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the FISMA evaluation for Fiscal Year (FY) 2019. CLA conducted its assessment based on: (1) the government-wide objective metrics prescribed by the Department of Homeland Security (DHS), which evaluate information security programs on a maturity scale from Level 1 (*Ad Hoc*) to Level 5 (*Optimized*) in eight IG FISMA Metric Domains and five Function areas; and (2) our judgmental assessment of the information security and privacy program, practices and controls for select systems in five security function areas.

The objective of this evaluation was to determine the effectiveness of the Corporation's information security program in accordance with FISMA, OMB requirements, and NIST guidance.

The information security program of the Corporation for National and Community Service (CNCS) has made little progress since last year, and it remains **NOT EFFECTIVE**. Most of the maturity metrics for the eight domains and five security functions remain unchanged. CNCS regressed in two of the domains and one of the function areas. Security training remains an area of strength at CNCS, but the good performance in this area is outweighed by the substantial risks resulting from the continuing control weaknesses in configuration management, identity and access management, and data protection and privacy.

The CNCS network continues to be exposed to critical and high severity vulnerabilities stemming from unpatched software, improper configuration settings and unsupported software. Most of these exist in servers and workstations associated with CNCS headquarters to include critical management servers. In addition, as of completion of our testing in August 2019, CNCS had not fully implemented multifactor authentication (use of a Personal Identification Verification (PIV) card along with user name and password) for all information system users and administrators. Management did not prioritize the implementation of multifactor authentication for privileged users as directed by OMB.

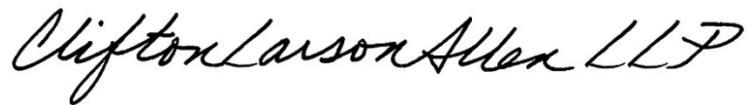
Furthermore, there are continuing deficiencies related to organization-wide risk management, configuration management, identity and access management, data protection and privacy, and logging and monitoring practices designed to protect mission-critical systems. These gaps limit the protection of CNCS's systems and data and may expose sensitive information, including Personally Identifiable Information, to unauthorized access and use.

We again recommend that CNCS complete 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 domains and security function 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. At the conclusion of our testing in August 2019, management indicated the plans for each function area were scheduled for completion on September 30, 2019.

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

A handwritten signature in black ink that reads "CliftonLarsonAllen LLP". The signature is written in a cursive, flowing style.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

TABLE OF CONTENTS

Executive Summary	1
FISMA Evaluation Findings	5
Security Function: Identify	5
1. CNCS Must Improve its Vulnerability and Patch Management Controls.....	5
2. CNCS Must Improve its Inventory Management Process	11
3. CNCS Must Fully Implement its Organization-wide Risk Management Program.....	12
Security Function: Identify Maturity Model Scoring	13
Security Function: Protect	15
4. CNCS Must Implement Standard Baseline Configurations	15
5. CNCS Must Implement Multifactor Authentication for Privileged and Non-Privileged Accounts	16
6. CNCS Must Strengthen Account Management Controls.....	18
7. CNCS Must Ensure All Information System Users Complete Access Agreements	21
8. CNCS Must Enhance the Personnel Screening Process	22
9. CNCS Must Strengthen Data Protection and Privacy Controls	23
10. CNCS Must Improve Physical Access Controls	25
Security Function: Protect Maturity Model Scoring	26
Security Function: Detect	28
11. CNCS Must Enhance the Review and Analysis of Wireless Network Audit Logs	28
Security Function: Detect Maturity Model Scoring	29
Security Function: Respond Maturity Model Scoring	30
Security Function: Recover Maturity Model Scoring	31

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Appendix I – Background..... 32

Appendix II – Scope and Methodology 36

Appendix III – Status of Prior Year Recommendations 39

Appendix IV – Management Comments..... 51

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

EXECUTIVE SUMMARY

The Federal Information Security Modernization Act of 2014 (FISMA)¹ requires Federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. The required standards are prescribed by the Office of Management and Budget (OMB) and the National Institute of Standards and Technology (NIST).

FISMA also requires each Inspector General to assess annually the effectiveness of the information security program at that Inspector General's agency. The Corporation for National and Community Service, Office of Inspector General (CNCS-OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the FISMA evaluation for Fiscal Year (FY) 2019. The objective of this evaluation was to determine the effectiveness of CNCS's information security program in accordance with FISMA, OMB requirements, and NIST guidance. CLA conducted its assessment based on: (1) the government-wide objective metrics prescribed by the Department of Homeland Security (DHS), which evaluate information security programs on a maturity scale from Level 1 (*Ad Hoc*) to Level 5 (*Optimized*) in eight IG FISMA Metric Domains and five Function areas; and (2) our judgmental assessment of the information security and privacy program, practices and controls for select systems in five security function areas.

We have determined that CNCS's information security program is **NOT EFFECTIVE**, because the five FISMA security function areas in its information security program and practices have not achieved sufficient maturity. To be considered effective, an agency's information security program must be rated *Managed and Measurable* (Level 4), on the five-point scale that ranges from *Ad Hoc* to *Optimized*.²

Overall, CNCS has made little progress in maturing its information security program since FYs 2017 and 2018. See Tables 1 and 2 below, comparing CNCS's maturity scores by security function and by domain for FY 2019 with those of FY 2017 and FY 2018. Most of the maturity metrics for the eight domains and five security functions remain unchanged from prior years.³ Since FY 2018, CNCS regressed in two of the domains and one of the function areas.

¹ The FISMA of 2014 (Public Law 113–283—December 18, 2014).

² The FY 2019 IG FISMA metrics align with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework [CSF]), version 1.1: Identify, Protect, Detect, Respond, and Recover.

³ CNCS's scored a four-way tie for the domains in the Protect function, ranging from *Ad Hoc* in configuration management to *Managed and Measurable* in security training. Because the algorithm defaults to the higher rating in the event of a tie, it rated CNCS as *Managed and Measurable* for the entire Protect function. To mitigate such anomalies, IGs have the discretion to determine the overall effectiveness rating and the rating for each of the Cybersecurity Framework functions at the maturity level of their choosing and explain the rationale for their effectiveness ratings. Here, we assessed the Protect function's maturity level as *Defined* (Level 2), because CNCS's good performance with respect to security training is outweighed by the severity of the control weaknesses in the other three domains: configuration management, identity and access management, and data protection and privacy. These control weaknesses leave CNCS's systems vulnerable to unauthorized access, loss of personally identifiable information and disruption.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Table 1: Comparison of Maturity Ratings in FY 2017, FY 2018, and FY 2019 by Function

Security Function⁴	Maturity Level by Function FY 2017	Maturity Level by Function FY 2018	Maturity Level by Function FY 2019
Identify	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Protect	Defined ⁵ (Level 2)	Defined ⁶ (Level 2)	Managed and Measurable ⁷ (Level 4) – <i>Calculated rating</i> Defined (Level 2) – <i>Assessed rating</i>
Detect	Defined (Level 2)	Defined (Level 2)	Ad Hoc (Level 1)
Respond	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	Defined (Level 2)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Overall	Not Effective	Not Effective	Not Effective

Table 2: Comparison of Maturity Ratings in FY 2017, FY 2018, and FY 2019 by Domain

Security Function⁸	IG FISMA Metric Domains	Maturity Level by Domain FY 2017	Maturity Level by Domain FY 2018	Maturity Level by Domain FY 2019
Identify	Risk Management	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Protect	Configuration Management	Defined (Level 2)	Defined (Level 2)	Ad Hoc (Level 1)
	Identity and Access Management	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
	Data Protection and Privacy	Not Included in FY 2017	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
	Security Training	Consistently Implemented (Level 3)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)
Detect	Information Security Continuous Monitoring	Defined (Level 2)	Defined (Level 2)	Ad Hoc (Level 1)
Respond	Incident Response	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	Contingency Planning	Defined (Level 2)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)

⁴ See Appendix I Table 4 and Table 5 for definitions and explanations of the Cybersecurity Framework Security Functions and metric domains.

⁵ The most frequent maturity level rating across the Protect CSF function served as the overall scoring.

⁶ The most frequent maturity level rating across the Protect CSF function served as the overall scoring.

⁷ See Note 3 for an explanation of the scoring of this function.

⁸ *Ibid* 3.

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FISCAL YEAR 2019 FISMA EVALUATION

CNCS faces ongoing challenges in the consistent implementation of its information security program and the monitoring of security controls. Our vulnerability scans identified more than 1,000 critical vulnerabilities and more than 6,500 high-severity vulnerabilities in the network, arising from unpatched software, improper configuration settings, and unsupported software. There are continuing deficiencies related to organization-wide risk management, configuration management, identity and access management, data protection and privacy, and logging and monitoring practices designed to protect mission-critical systems. These gaps limit the protection of CNCS's systems and data and may expose sensitive information, including Personally Identifiable Information (PII), to unauthorized access and use.

There has been progress made in closing prior recommendations; since last year, CNCS has closed 21 of the 46 open recommendations from the FY 2014 – FY 2018 FISMA evaluations, reflecting improvements in security authorization; system risk assessments; testing and documentation of system changes; and aggregating the Momentum⁹ Oracle database security logs into the security event management system (*i.e.*, Splunk tool). CNCS also began implementation of multifactor authentication; however, the process was not fully implemented when our testing concluded in August 2019.

However, CNCS continues to lack a strategic approach that will achieve effective information security within a reasonable period. Among the 25 prior recommendations that remain unimplemented are the critical recommendations to analyze the IG metrics and develop a plan for the steps necessary to make steady, measurable improvement towards reaching an effective information security program (Level 4, *Managed* and *Measurable*) for each function area.¹⁰ At the conclusion of our testing in August 2019, management indicated the plans for each function area were scheduled for completion on September 30, 2019.

To address the continuing weaknesses in CNCS's information security program and practices, we have provided 33 recommendations - 22 new, 3 modified, and 8 repeats - that will assist CNCS in addressing challenges in its development of a mature and effective information security program.

Management's Response and Evaluator's Comments

In response to the draft report, CNCS concurred with, and its planned actions are responsive to, 31 of the 33 recommendations. CNCS concurred in part with Recommendation 8 and indicated plans to take certain corrective actions. CNCS disagreed with Recommendation 15 and does not intend to take further action on it.

Recommendation 8 is that CNCS continue its current effort to complete a comprehensive risk register at the mission- and business-process level. CNCS stated that it has an Enterprise Risk Register, which was created by identifying and assessing risk at the business process level, as well as the enterprise level. However, this risk register represented CNCS's first attempt to identify its risks. The business process information was gathered in FY 2016, had not been updated and was no longer being used by CNCS to support risk-based decisions. During our fieldwork, the Office of the Chief Risk Officer (OCRO) advised that it was working internally with other CNCS offices and implementing a new process to develop a mission- and business-

⁹ The CNCS's financial system.

¹⁰ Refer to Appendix III for a list of open recommendations from the OIG's prior FISMA evaluations.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

process level risk register based on current information. Accordingly, Recommendation 8 will remain open until we can validate the implementation of the proposed corrective action.

Recommendation 15 pertains to the need to ensure that the Momentum application, which CNCS uses for financial management, is recertified quarterly, that is, to confirm that users are properly authorized to access this critical application. CNCS asserts that its continuous monitoring includes Momentum account recertification, in that any missed recertifications are documented and reported to the Authorizing Official. However, this process includes no control to ensure that, upon receipt of such a report, the Authorizing Official takes corrective action to complete the missed recertification.

CNCS also states that its planned migration of accounting functions to a shared services provider will mitigate the risks of missed recertifications for Momentum users. However, the migration is not scheduled to occur until FY 2021, and CNCS will continue to rely on Momentum throughout FY 2020. Thus, the risks of improperly certified access to Momentum will persist throughout the current fiscal year. We therefore recommend that CNCS revises its corrective action to address this issue.

CNCS's comments are included in their entirety in Appendix IV. The FY 2020 FISMA evaluation will include an assessment of CNCS's implementation of corrective actions, including a determination which of them can be closed.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

FISMA Evaluation Findings

The findings identified in this evaluation align with the particular security domains, as summarized in **Table 3** which details the findings mapped to the IG FISMA Metric Domains.

Table 3: Cybersecurity Framework Security Functions mapped to weaknesses noted in the FY 2019 FISMA Evaluation of CNCS

FY 2019 IG FISMA Metric Domain	FY 2019 Weaknesses
Risk Management	Unpatched and unsupported software (Finding 1)
	Lack of information system asset inventory management (Finding 2)
	Lack of a mission and business risk registry (Finding 3)
Configuration Management	Configuration baselines not fully implemented (Finding 4)
Identity and Access Management	Lack of multifactor authentication (Finding 5)
	Insufficient account management controls (Finding 6)
	Lack of information system user access agreements (Finding 7)
	Insufficient personnel screening process (Finding 8)
	Inadequate physical controls (Finding 10)
Data Protection and Privacy	Lack of Protection of Personally Identifiable Information (Finding 9)
Information Security Continuous Monitoring	Inadequate review and analysis of audit logs (Finding 11)

The following section provides a detailed discussion of the findings grouped by the Cybersecurity Framework Security Functions.

Security Function: Identify

1. CNCS Must Improve its Vulnerability and Patch Management Controls

FY 2019 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. However, the CNCS network continues to be exposed to critical and high severity vulnerabilities through unpatched software, improper configuration settings, and unsupported software. While our independent vulnerability scans indicated that the number of vulnerabilities has decreased slightly since last year, the remaining vulnerabilities continue to be high in volume as well as in severity **(Figures 1 and 2)**.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

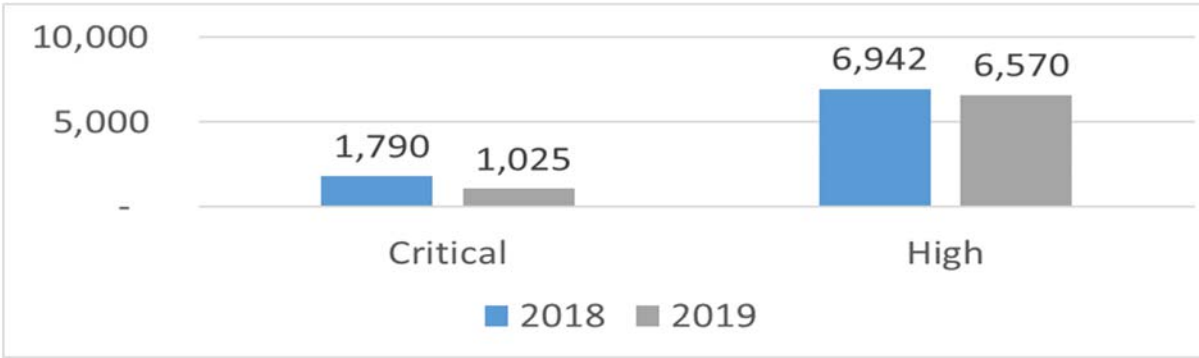


Figure 1. Comparison of the total number of vulnerabilities identified by the independent auditors' vulnerability scans from FY 2018 and 2019.

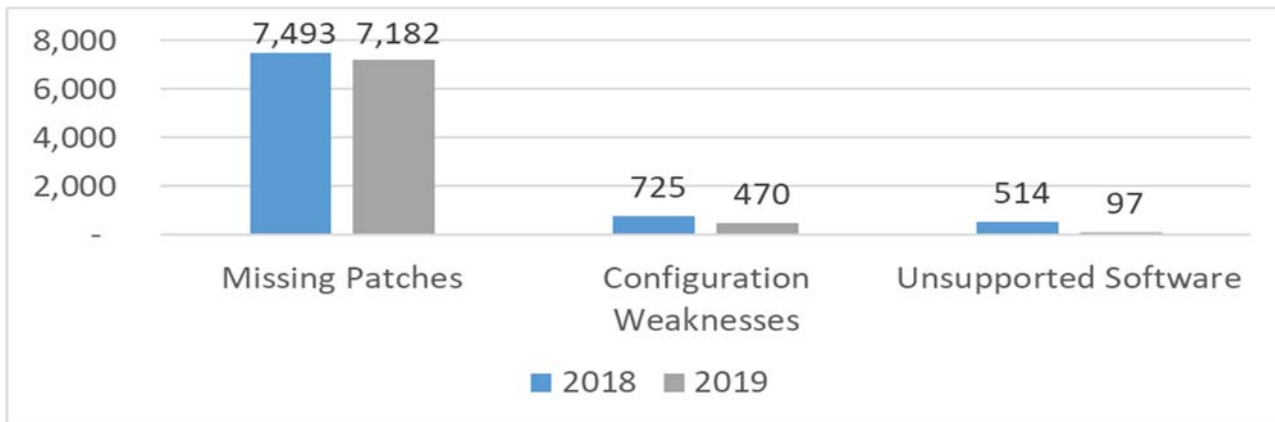


Figure 2. Comparison of the total number of vulnerabilities by type identified by the independent auditors' vulnerability scans from FY 2018 and 2019.

Specifically, we noted patch management issues at four CNCS locations: Headquarters (HQ), Washington, DC; National Civilian Community Corps (NCCC) Pacific Region Campus and its computer lab at Sacramento, CA; and NCCC Southwest Region Campus at Denver, CO:

- CNCS Headquarters: From a scan¹¹ of 169 servers and 199 workstations at the CNCS Washington, D.C., HQ, we identified **898 critical and 6,390 high-risk vulnerabilities** related to patch management, configuration management, and unsupported software. Of the 7,288 total critical and high vulnerabilities, 6,748 were caused by missing patches, 450 were caused by configuration weaknesses, and 90 were caused by unsupported software. **Figures 3 and 4** depict CNCS HQ vulnerabilities by criticality and type.

¹¹ Based on independent auditors' scans using the Tenable Nessus Vulnerability Scanner software tool.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

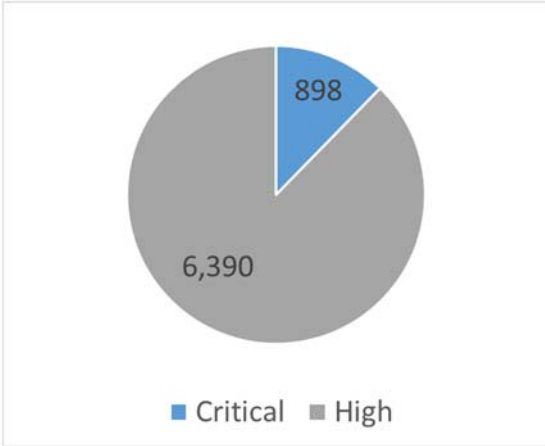


Figure 3 HQ total vulnerabilities by criticality



Figure 4 HQ total vulnerabilities by type

- NCCC Pacific Region Campus: Based on independent scans of 17 computing devices on the CNCS network, we identified **81 critical and 171 high-risk vulnerabilities** related to patch management, configuration management, and unsupported software at the NCCC Pacific Region Campus. Of the 252 total critical and high vulnerabilities, 240 were caused by missing patches, 11 were caused by configuration weaknesses, and 1 was caused by unsupported software. **Figures 5 and 6** depict NCCC Pacific Region Campus total vulnerabilities by criticality and type.

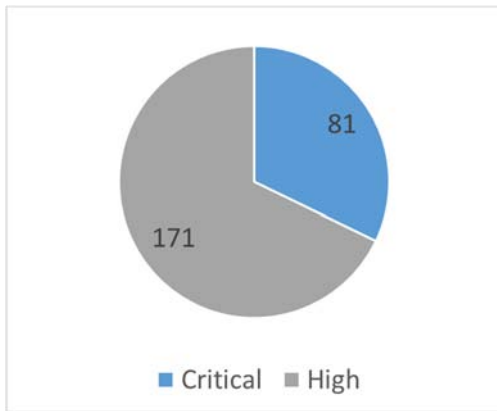


Figure 5 NCCC Pacific Region Campus total vulnerabilities by criticality



Figure 6 NCCC Pacific Region Campus total vulnerabilities by type

- NCCC Pacific Region Campus computer lab: Based on independent scans of 10 computing devices, we identified **61 critical and 286 high-risk vulnerabilities** related to patch management, configuration management, and unsupported software at the NCCC Pacific Region Campus computer lab. Of the 347 total critical and high vulnerabilities, 288 were caused by missing patches, 47 were caused by configuration weaknesses, and 12 were caused by unsupported software. The computers in the NCCC Pacific Region Campus computer lab are not connected to the CNCS network and are managed by staff on-site. **Figures 7 and 8** depict NCCC Pacific Region Campus computer lab total vulnerabilities by criticality and type.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

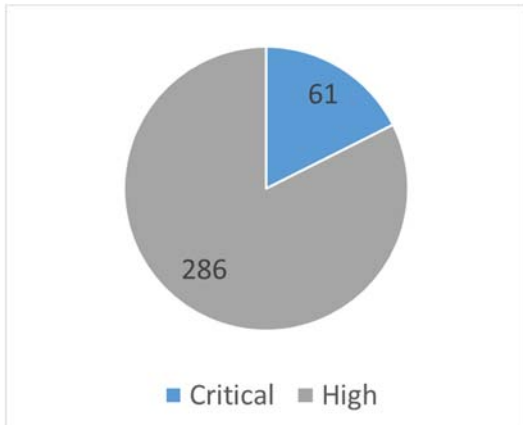


Figure 7 NCCC Pacific Region Campus computer lab total vulnerabilities by criticality

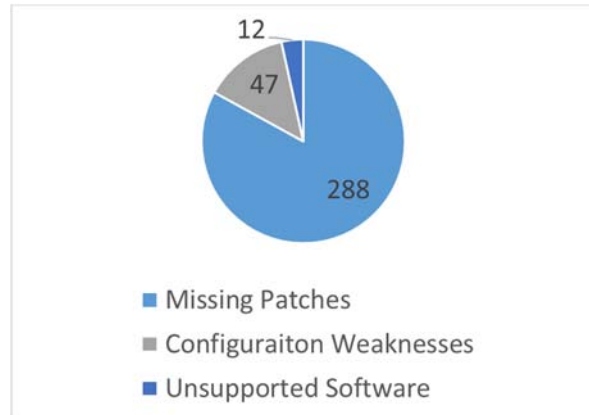


Figure 8 NCCC Pacific Region Campus computer lap total vulnerabilities by type

- NCCC Southwest Region Campus: Based on independent scans of 12 computing devices on the CNCS network, we identified **46 critical and 163 high-risk vulnerabilities** related to patch management, configuration management, and unsupported software at the NCCC Southwest Region Campus. Of the 209 total critical and high vulnerabilities, 194 were caused by missing patches, nine were caused by configuration weaknesses, and six were caused by unsupported software. **Figures 9 and 10** depict NCCC Southwest Region Campus total vulnerabilities by criticality and type.

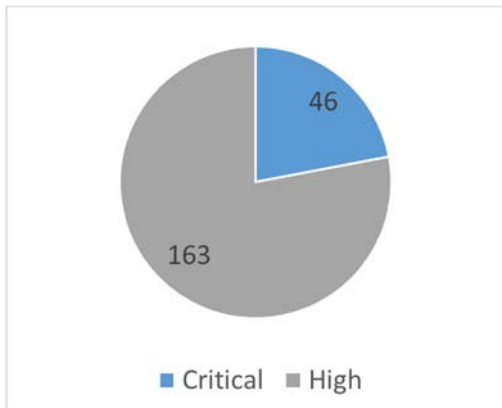


Figure 9 NCCC Southwest Region Campus total vulnerabilities by criticality



Figure 10 NCCC Southwest Region Campus total vulnerabilities by type

- Seventy-three percent of the patch management vulnerabilities from both NCCC campuses and CNCS HQ were publicly known before 2018, such as those related to Adobe Acrobat, Adobe Flash Player, Oracle, and Windows security patches.
- All of the configuration weaknesses were publicly-known before 2018 and were related to required registry changes for Windows Patches, Server Message Block being insecurely configured, and Simple Network Management Protocol default community names.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

- The unsupported software was related to the following (including but not limited to):
 - Microsoft Exchange Server (no longer supported as of July 12, 2011) was identified at HQ.
 - Microsoft XML Parser and XML Core Services (no longer supported as of April 12, 2014) was identified at HQ.
 - VMware ESX/ESXi (no longer supported as of May 21, 2014) was identified at HQ.
 - Adobe Flash Player (no longer supported as of June 1, 2014) was identified at HQ.
 - Adobe Photoshop (no longer supported as of February 2015) was identified at the NCCC Southwest Region Campus.
 - Microsoft SQL Server (no longer supported as of July 14, 2015) was identified at HQ.
 - McAfee VirusScan Enterprise (no longer supported as of December 31, 2015) was identified at HQ.

Furthermore, the dedicated command and control management terminal servers used by the CNCS IT services vendor to remotely access the CNCS network and manage its network devices, deploy patches to servers, laptops, workstations, and other network devices themselves had a significantly high number of critical and high vulnerabilities. Comparatively, these management servers used by their vendor to access their network had more vulnerabilities on average putting CNCS and its data at an increased risk of compromise. CNCS officials were unaware of the risk because they had limited access to these management servers, which were not part of the monthly CNCS vulnerability scans.

Additionally, there was a wireless printer in use that is no longer supported by the vendor at the NCCC Pacific Region Campus. The old Hewlett Packard plotter/printer with wireless networking enabled at the NCCC Pacific Region Campus was not on the HQ inventory; therefore, Office of Information Technology (OIT) personnel did not know the printer was still in use.

The overall deployment of vendor patches and system upgrades to mitigate the vulnerabilities was decentralized, inconsistent, and not effective across all networks and facilities. In addition, there was no process in place to ensure the timely correction of identified information system flaws, such as configuration weaknesses or unsupported software. Further, the internet bandwidth available to both the NCCC Pacific Region Campus and NCCC Southwest Region Campus was not sufficient to allow for all patches to be installed on CNCS computers during a routine patch cycle. There were significant internet disruptions at both campuses, while the audit team was on-site, as patches were being pushed out of cycle to the devices during the day of our site visits.

Also, the FY 2018 FISMA evaluation report¹² included two recommendations to assist CNCS to improve their vulnerability management process. At the conclusion of our testing in August 2019, management stated that the remediation of these two recommendations was still on-going with a target completion date of September 30, 2019 for Recommendation 1 and September 2023 for Recommendation 2.

¹² Recommendations 1 and 2, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 198-03, March 1, 2018).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Finally, management stated that the OIT infrastructure personnel did not review vulnerability scan results in Tenable Security Center, the vulnerability analysis tool because there was no request to have accounts created. This resulted in management not being able to effectively monitor the vulnerability management activities of the contractor to ensure patches were timely deployed in accordance with CNCS policy.

The CNCS *Cybersecurity Control Families* document states that the Information System Security Officer (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 7 days
 - High - within 30 days
 - Moderate - within 90 days
 - Low - within 180 days
- Sharing information obtained from the vulnerability scanning process and security control assessments with Cybersecurity to help eliminate similar vulnerabilities in other information systems (*i.e.*, systemic weaknesses or deficiencies)

The systems at the NCCC Pacific Region Campus, NCCC Southwest Region Campus and CNCS HQ are at elevated risk due to unpatched systems. A variety of critical vulnerabilities could be exploited using unsophisticated techniques to take control of systems, cause a denial of service attack, or allow unauthorized access to the CNCS systems and applications. In addition, operating system and application software with missing security patches or outdated security patches could leave security weaknesses exposed to increased attack methods that compromise the confidentiality, integrity, and availability of data.

Additionally, by CNCS OIT personnel not having access to review the vulnerability scan results, CNCS is not able to monitor and manage the contractor to ensure remediation actions are being performed in accordance with CNCS policy.

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

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.*
- *Replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer.*
- *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.*

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

- *Enhance the inventory process to ensure all devices are properly identified and monitored. (Repeat)¹³ (FY19 – FISMA – NFR 11)*

Recommendation 2: *Ensure that OIT evaluates if the internet connections at the National Civilian Community Corps Campuses and Regional 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. (Modified Repeat) (FY19 – FISMA – NFR 11)*

Recommendation 3: *Create accounts for CNCS OIT's Infrastructure staff identified by the Director of Infrastructure for monitoring the vulnerability scanning tool and validating vulnerability management activities on the networks and devices they manage. (New) (FY19 – FISMA – NFR 11)*

2. CNCS Must Improve its Inventory Management Process

FY 2019 IG FISMA Metric Area: Risk Management

CNCS did not effectively manage its information system asset inventory. Applying adequate security controls to CNCS IT assets requires knowing what those assets are and where they are located. However, we noted the following issues related to the completeness and accuracy of the inventory:

- Five of 20 judgmentally sampled IT assets from the NCCC Southwest Region Campus listed on the OIT HQ information system asset inventory Configuration Management Database (CMDB) were inaccurate. Specifically:
 - The asset tag number of an OIT switch was incorrectly listed in the OIT HQ inventory. Upon notification of the issue, OIT management corrected the asset tag number in the inventory listing.
 - Three printers listed on the HQ inventory, as belonging to the NCCC Southwest Region Campus were no longer found at the campus. In addition, two of the three printers did not have RemedyForce tickets, which are used at field site locations for tracking inventory changes, or updates associated with their current location in the FasseTrack system.¹⁴
 - One laptop was incorrectly listed as located in the NCCC Southwest Region; however, the laptop was assigned to an individual in the NCCC Pacific Region Campus. Upon notification of the issue, OIT management corrected the inventory to state the location was the NCCC Pacific Region Campus.
- From the total population of 464 assets listed on the NCCC Pacific Region Campus IT asset inventory, 106 assets were not listed on the HQ IT inventory.
- NCCC Pacific Region Campus Laptops for 9 out of 21 NCCC Pacific Region Campus employees were not listed on the HQ IT asset inventory.

¹³ Repeat means that the prior year recommendation remains open.

¹⁴ FasseTrack is an asset management system for electronic tracking and maintenance of inventory.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

- From the total population of 197 NCCC Pacific Region Campus items, three assets had an incorrect location or individual ownership information on the HQ IT asset inventory.

OIT stated that the current inventory management process is predominantly manual and involves HQ personnel updating the CMDB inventory and the FasseTrack system when changes occur. This manual process introduces a greater risk of errors when updates are not made timely or correctly in both systems. Management also stated that manual updates were not consistently made to the CMDB inventory by HQ personnel, and to the FasseTrack system by NCCC personnel, at the time the inventory was updated. In addition, RemedyForce tickets were not consistently completed on a real-time basis. Management indicated that in the next twelve to eighteen months, OIT will directly manage IT assets for all NCCC campuses by using CMDB only. Management also stated that it is looking for a more automated inventory process; however, an automated solution has not been selected or approved for purchase.

The CNCS *Cybersecurity Control Families* document requires the information system component inventory to be reviewed and updated at least annually.

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

To assist CNCS in strengthening information system component inventory management controls, we recommend that CNCS:

Recommendation 4: *Develop and implement a written process to ensure manual updates to the CMDB inventory and FasseTrack system are made simultaneously when the inventory is updated. (New) (FY19 – FISMA – NFR 6)*

Recommendation 5: *Develop and implement a written process to ensure RemedyForce tickets are completed at the time the inventory is updated. (New) (FY19 – FISMA – NFR 6)*

Recommendation 6: *Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system. (New) (FY19 – FISMA – NFR 6)*

Recommendation 7: *Perform and document analysis to determine the feasibility of completely automating the inventory management process. (New) (FY19 – FISMA – NFR 6)*

3. CNCS Must Fully Implement its Organization-wide Risk Management Program

FY 2019 IG FISMA Metric Area: Risk Management

CNCS created an information system risk register; however, it did not develop a risk register to record identified risks at the mission and business process level as defined by NIST. Specifically, NIST specifies an integrated three-tiered approach to risk management that addresses risk at the

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

organization level, mission and business process level, and information system level.¹⁵ The FY 2018 FISMA evaluation report¹⁶ made recommendations for CNCS to develop and document a comprehensive risk register at the mission and business process level and ensure the information system risk register included all NIST required risk assessment elements.

Management stated that the OCRO had gathered risk information from all of CNCS's offices to support the enterprise-level risk register in FY 2016. However, the business process level information gathered back in FY 2016 became outdated and was no longer being used to support risk-based decisions. Therefore, OCRO is working internally with other CNCS offices and implementing a new process to develop a mission and business process level risk register, with the expected completion date of December 2019.

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 the likelihood of harm occurring)."

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

Since the prior year recommendation was not completed, we made the same recommendation this year to assist CNCS in continuing to strengthen the risk management process. We recommend CNCS:

Recommendation 8: *Continue the current effort to complete a comprehensive risk register at the mission and business process level. (Repeat) (FY19 – 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 Level 2 (*Defined*), Not Effective, as depicted in the chart below:

Function	Count	IG FISMA Metric Questions
Ad Hoc (Level 1)	0	NA
Defined (Level 2)	5	2, 5, 7, 10, and 12
Consistently Implemented (Level 3)	2	9, and 11

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."

¹⁶ Recommendations 4 and 5, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 18 (OIG Report No. 19-03, March 1, 2019).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Function	Count	IG FISMA Metric Questions
Managed and Measurable (Level 4)	4	1, 3, 6, and 8
Optimized (Level 5)	1	4
Calculated Maturity Level: Defined (Level 2), Not Effective		

The *FY 2019 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 mission and risks faced, risk appetite, and risk tolerance level.

The FY 2018 FISMA evaluation report¹⁷ included a recommendation for CNCS to perform an analysis of the IG FISMA Metrics related to the security function “Identify” and develop a multi-year strategy that addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. At the conclusion of our testing in August 2019, management indicated September 30, 2019, as the date for completion.

Since the prior year recommendation was not completed, we made the same recommendation this year to assist CNCS in reaching an effective rating for the “Identify” function area. We recommend CNCS:

Recommendation 9: *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. (Repeat)*

¹⁷ Recommendation 7, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 18 (OIG Report No. 19-03, March 1, 2019).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Security Function: Protect

4. CNCS Must Implement Standard Baseline Configurations

FY 2019 IG FISMA Metric Area: *Configuration Management*

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

CNCS did not document standard baseline configurations for all databases, network devices, VMware ESX hosts, and Web browsers. Although there was a baseline documented for the Windows Server 2008, CNCS did not develop exact guidelines used to create the baseline. Specifically:

- The *Corporation for National and Community Service Baseline Configuration Standard* explicitly states “[t]he standard in use for Windows Server 2008 R2 is an organizational legacy standard, which was inherited by current administrative staff. It is based on a historical NIST guideline for Windows Server 2008 R2, however, the exact guideline is unknown.”
- Our independent network scans noted compliance of only 62 percent for Windows Server 2012 machines on the CNCS network. We used the Windows Server 2012 Center for Internet Security (CIS)¹⁸ Level 1 benchmark to assess baseline compliance - as noted in the *Corporation for National and Community Service Baseline Configuration Standard*.

This occurred because, in FY 2018, management decided that it would not implement the CIS baselines on its IT platforms. The Chief Information Security Officer (CISO) stated that CNCS developed its own baselines based on vendor’s recommendations and the estimated completion date would be September 30, 2019. Upon notification of the discrepancy in the *CNCS Cybersecurity Control Families* document related to the vendor’s recommended baseline, the CISO updated it to reflect CNCS approval of vendor baselines.

As noted in the *CNCS Service Baseline Configuration Standard*, the Windows Server 2008 guideline is unknown due to prior management decisions. Due to the impending end of life of Windows Server 2008 on January 14, 2020, management decided to continue the operation of the current devices until they can be migrated to a newer platform. According to management, all of the end-of-life servers will be upgraded by the end of December 2019.¹⁹ In addition, the Windows Server 2012 machines were not brought into compliance because of other higher priority tasks, such as the rollout of Windows 10.

¹⁸ Center for Internet Security maintains "The CIS Controls," a popular set of 20 security controls "which map to many compliance standards." CIS provides global standards for internet security and is a recognized global standard and best practices for securing IT systems and data against attacks. www.cisecurity.org.

¹⁹ A recommendation to ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer was made in Finding 1 related to vulnerability management.

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FISCAL YEAR 2019 FISMA EVALUATION

Further, the FY 2017²⁰ and FY 2018²¹ FISMA evaluations included recommendations for CNCS to ensure standard baseline configurations for all platforms in the CNCS IT environment are appropriately implemented, tested, and monitored for compliance with established CNCS security standards. Management did not take corrective action to address these recommendations in FY 2019.

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.

In addition, the *CNCS Cybersecurity Control Families* document requires the ISSO to establish, document, implement, and monitor standard baseline configuration settings.

Information technology components that do not comply with standard baseline configurations increase the risk of a security vulnerability being exploited. In addition, without monitoring for compliance with standard baseline configurations, configurations may be intentionally or inadvertently altered from the approved baseline without management's knowledge making the detection, response, and recovery from unauthorized access difficult to appropriately manage.

To assist CNCS in continuing to strengthen the configuration management program, we recommend that CNCS:

Recommendation 10: *Establish and document standard baseline configurations for all platforms in the CNCS information technology environment and ensure these standard baseline configurations 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) (FY19 – FISMA – NFR 9)*

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

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

CNCS did not implement multifactor authentication²² (e.g. PIV card) for local and network access for privileged users.²³ In addition, although multifactor authentication for network access was being implemented for non-privileged users on Microsoft Windows 10 workstations in July 2019, it was not fully enforced. Users were still able to log in with just a user name and password. Further, at the conclusion of field testing, there were non-privileged users still using Windows 7 workstations for which multifactor authentication was not implemented. For example, our network scans indicated there was one Windows 7 workstation at CNCS HQ, nine Windows 7 workstations

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

²¹ Recommendations 8, 9 and 10, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 20, (OIG Report No. 19-03, March 1, 2019).

²² 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.

²³ Privileged users are have administrative access to information systems allowing for modification of system configurations, installing and removing software, and other security-related functions.

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FISCAL YEAR 2019 FISMA EVALUATION

at the NCCC Southwest Region Campus, and 11 Windows 7 workstations at the NCCC Pacific Region Campus.

Management did not prioritize the implementation of multifactor authentication for privileged users as directed by OMB. At the conclusion of our testing in August 2019, management indicated that the infrastructure for PIV implementation for privileged users was completed and tested, and the scheduled implementation date was September 30, 2019. Currently, multifactor authentication is only enforced for remote access to the CNCS network. The FY 2017²⁴ and FY 2018²⁵ FISMA evaluations included recommendations for CNCS to implement PIV multifactor authentication for local and network access for privileged users and implement PIV multifactor authentication for network access for non-privileged users. Based on our review, we noted that the recommendations were not fully completed and remain open.

Multifactor authentication for non-privileged users was not fully enforced because management granted a grace period of 60 days after the deployment date of July 15, 2019 for users to still log in with a user name and password without a PIV card. This decision was made so that users offsite or on travel would not be adversely affected during the multifactor authentication implementation. Management also stated that the users whose workstations were not upgraded to Windows 10 were either remote, on travel, or on leave, and the upgrades will be completed once all of the new regional offices are established. At the conclusion of our testing in August 2019, management indicated that PIV multifactor authentication would be fully enforced for non-privileged users by September 15, 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*, (October 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. According to OMB's June 12, 2015 release, *Enhancing and Strengthening the Federal Government's Cybersecurity*, federal agencies were instructed to dramatically accelerate the implementation of multi-factor authentication, especially for privileged users.

Without strong multifactor authentication for network access for non-privileged user accounts, there is an increased risk of unauthorized access to CNCS information and information systems by an unauthorized user, decreasing data confidentiality and integrity. The risk is greater when strong multifactor authentication is not implemented for local and network access for privileged user accounts. Unauthorized privileged access can allow an individual to inappropriately create, delete and modify users and services running on the network, as well as gain access to all data

²⁴ Recommendations 14 and 15, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 23, (OIG Report No. 18-03, December 18, 2017).

²⁵ Recommendations 11 and 12, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 22, (OIG Report No. 19-03, March 1, 2018).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

stored on the network. As a result, CNCS may be exposed to inappropriate or unauthorized access to sensitive information, including Personally Identifiable Information (PII), which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

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 to all workstations and servers. (Modified Repeat)²⁶ (FY19 – FISMA – NFR 8)*

Recommendation 12: *Complete the implementation of Personal Identification Verification multifactor authentication for network access for all non-privileged users by upgrading all users to Microsoft Windows 10 workstations and enforcing logon with a Personal Identification Verification card. (Modified Repeat) (FY19 – FISMA – NFR 8)*

6. CNCS Must Strengthen Account Management Controls

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

CNCS did not effectively manage user accounts and/or passwords for the network. For example, CNCS officials did not disable network accounts of separated employees and inactive accounts, perform reviews of account users' roles and permissions, and properly manage passwords that were not changed after a designated timeframe specified in CNCS policies. 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.

Specifically, the following issues were noted:

Weaknesses in Account Management of Separated Employees:

- Twenty-two of 65 federal employees who separated between November 27, 2017, and April 13, 2019; and 2 of 27 contractors who separated between January 9 and February 2, 2019, still had their Momentum accounts active as of May 10, 2019. Management stated that an automated capability was not implemented to disable Momentum accounts that passed their defined "End Date." Upon notification of this issue, CNCS implemented a nightly script in the system to deactivate accounts that passed their defined "End Date."
- Two of the 65 separated federal employees, whose network accounts had been disabled, still had active access to the My AmeriCorps Staff Portal AD Organizational Unit (OU),²⁷ including separated employees as far back as April 2019. Management stated that it did not implement a process to remove My AmeriCorps Staff Portal OU accounts when employees separated from CNCS. Upon notification of this issue, CNCS implemented a script in the system to flag separated employees' accounts for removal in the Staff Portal

²⁶ Modified Repeat means part of the condition, cause, or recommendation have changed from the prior year finding due to some progress made by CNCS.

²⁷ An OU is a subdivision in Active Directory to hold users, groups, and computers with designated Group Policy settings and account permissions.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

OU. Without disabling separated users' system accounts, there is a risk that these accounts could be accessed by unauthorized users.

Improper Management of Inactive Accounts:

- Twenty-eight non-privileged and three privileged users did not log in to the CNCS network within 30 days, but their network accounts were not disabled in accordance with CNCS policy. Management did not implement an automated means to capture network accounts that reached both 90 days without a password change and 30 days of inactivity. Upon notification of this issue, CNCS implemented a script in the system to automatically detect and disable these inactive accounts going forward.

In addition, CNCS placed the privileged network accounts in a separate OU, for which Group Policy did not require the privileged users to change their passwords or log in the network upon a defined timeframe. Unauthorized users could use a dormant account to gain access to CNCS's information systems. Upon notification of this issue, management modified the Group Policy for privileged accounts to enforce the CNCS policy on account inactivity. Although inactive user accounts are dormant, they still retain access to systems and data, posing a target for potential exploitation.

- Thirty-four My AmeriCorps Staff Portal accounts that were created between 2003 and March of 2019 were never logged in, and these accounts were not removed from the My AmeriCorps Staff Portal AD OU. Management stated that an erroneous system script was utilized to disable inactive My AmeriCorps Staff Portal accounts and CNCS did not properly monitor the system script. If the separated individual's disabled network accounts are not removed from the AD My AmeriCorps Staff Portal OU, and the AD accounts are purposefully or inadvertently re-enabled, these accounts can be used to access the My AmeriCorps Staff Portal.

Lack of Account Review/Recertification:

- CNCS did not perform recertification of Momentum user accounts during the first two quarters of FY 2019 as required by the CNCS policy. Management stated that this occurred due to changes in ownership and responsibility for Momentum during FY 2019. Without a periodic review of information system users' account roles and permissions, there is an increased risk that least-privilege access is not maintained, and individuals may have more access than they should to perform their job duties. This could lead to users inappropriately modifying or disclosing sensitive information.

Weaknesses in Password Management:

- Thirty-three non-privileged and five privileged network account users did not change their account password within 90 days and their accounts were not disabled in accordance with CNCS policy. Upon notification of this issue, management modified the Group Policy for privileged accounts to follow CNCS policy on password management.
- Thirteen eSPAN account users did not change their account password within 60 days and their accounts were not disabled as required by the eSPAN System Security Plan. Management stated the eSPAN password configuration setting was incorrectly set to 180 days instead of the 60-day password requirement and management did not monitor the configuration settings. Without changing passwords periodically, there is an increased risk that unauthorized users targeting these accounts might have access to the accounts. Regular password changes limit the period of exposure to sensitive CNCS should the account be compromised. Upon notification of this issue, CNCS modified the configuration to the correct setting.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

The CNCS *Cybersecurity Control Families* document requires the following regarding disabling accounts for separated employees, disabling inactive accounts and managing passwords:

- The Information Security Officer (ISO), upon the termination of individual employment, is responsible for ensuring information system access is disabled within one (1) working day following termination action.
- The Information System Security Manager or an individual designated by the ISO is responsible for ensuring the information system automatically disables inactive accounts after 30 days.
- The Information System Security Manager or an individual designated by the ISO is responsible for reviewing accounts for compliance with account management requirements at least quarterly.
- The ISSO is responsible for managing information system authenticators by changing/refreshing authenticators every 90 days.

Without effective management of user accounts and passwords, CNCS information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure.

To assist CNCS in strengthening the management of information system user accounts and passwords, we recommend CNCS:

Recommendation 13: *Develop and implement a written process for the Director of Infrastructure to monitor the employee separation process to ensure CNCS policy is followed for disabling system accounts within one working day following separated employees' termination and disabled network accounts of separated individuals are removed from the Active Directory My AmeriCorps Staff Portal Organizational Unit. (New) (FY19 – FISMA – NFR 1)*

Recommendation 14: *Enhance information systems to automatically disable user accounts after 30 days of inactivity in accordance with CNCS policy. This includes monitoring automated scripts to validate accounts are disabled properly. (New) (FY19 – FISMA – NFR 1)*

Recommendation 15: *Develop and implement a written process for the Chief Information Security Officer to ensure an account quarterly review/recertification is performed for Momentum. (New) (FY19 – FISMA – NFR 1)*

Recommendation 16: *Develop and Implement a written process that ensures all CNCS information system passwords are changed at the frequency specified in applicable CNCS policy or the System Security Plan. (New) (FY19 – FISMA – NFR 1)*

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

7. CNCS Must Ensure All Information System Users Complete Access Agreements

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

CNCS did not ensure all Momentum, eSPAN, and My AmeriCorps Staff Portal users completed system access agreements (Rules of Behavior) prior to gaining system access. Specifically, we noted that two out of eight sampled new Momentum users, one out of three sampled new eSPAN users, and two out of three sampled new My AmeriCorps Staff Portal users selected for testing²⁸ did not complete a signed Rules of Behavior per CNCS Cybersecurity Policy. User access agreements require information system users to acknowledge and agree to rules of behavior for accessing CNCS's information systems. User access agreements should be completed prior to gaining access to CNCS's information systems and recertified periodically thereafter.

Management stated that it was a lack of oversight on new system users who did not complete Rules of Behavior prior to gaining system access. Therefore, the ISO did not validate that the Rules of Behavior were completed prior to granting the user system access. Upon notification of the issue, management followed up with those identified users to complete their Rules of Behavior.

NIST SP 800-53, Revision 4, requires organizations to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access. The CNCS *Cybersecurity Control Families* also requires the ISO to ensure that individuals requiring access to organizational information and information systems sign appropriate access agreements prior to being granted access.

Without ensuring new information system users complete access agreements prior to gaining system access, there is an increased risk that system users do not understand their responsibilities when accessing CNCS's information systems and managing CNCS data. Requiring the completion of the Rules of Behavior ensures that users read, understand, and agree to follow the rules and limitations related to the access to their authorized systems.

To assist CNCS in strengthening personnel security controls related to accessing information systems, we recommend CNCS:

Recommendation 17: *Develop and implement a written process for the Information Security Officer to validate that all new information system users complete the Rules of Behavior prior to gaining system access in accordance with CNCS policy. (New) (FY19 – FISMA – NFR 2)*

²⁸ The information systems under the scope of the FY 2019 FISMA evaluation included the General Support System, Momentum, eSPAN, and My AmeriCorps Portal. The users who did not complete signed Rules of Behavior were a sample of users tested, but not the entire population of new users.

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FISCAL YEAR 2019 FISMA EVALUATION

8. CNCS Must Enhance the Personnel Screening Process

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

CNCS did not ensure employees had the proper background investigations. 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 CNCS. Therefore, CNCS must consider a risk designation based on the sensitivity level of the position when it screens its employees and contractors. Specifically, we noted the following issues:

- Three of the five sampled GSS privileged users had background investigations at a lower level than the risk associated with their assigned positions, as noted in the Position Designation Record (PDR).²⁹ These individuals had Tier 2 investigations and the investigation levels required on the PDRs were Tier 4 investigations.³⁰
- In addition, Office of Human Capital (OHC) was unable to validate whether two Momentum privileged users, who were contractors, had completed background investigations.

Additionally, the FY 2018 FISMA evaluation identified 11 from a sample of 23 employees with access to the CNCS network and eSPAN, whose background investigations were below the required level than the risk associated with their assigned positions as noted in their PDR. These individuals had a Tier 1 investigation and the investigation level required on the PDRs were Tier 2 and Tier 4 investigations. Eight of the 11 employees identified in the FY 2018 FISMA evaluation still had background investigations below their required levels.

Furthermore, the investigation levels for two of the three sampled privileged Momentum users identified in the FY 2017 FISMA evaluation were still below the level commensurate with the risk associated with their assigned positions. These individuals had National Agency Check with Inquiries (NACI) or Tier 1 investigations. The privileged Momentum users were assigned sensitive roles and system application permissions that would require a higher level of background investigation. They had the ability to add, modify and delete their own and other Momentum users' roles and permissions.

The FY 2018 FISMA evaluation³¹ included recommendations for CNCS to perform and document an assessment of staffing and funding levels required for background investigations and address any recognized gaps, and develop, document and implement a schedule to prioritize background investigations for individuals with higher-level risk as noted in the PDR. Although the investigations are not yet completed, CNCS had completed an assessment of staffing and funding requirements for background investigations. Additionally, CNCS had developed a schedule to prioritize background investigations based on position risk. Therefore, CNCS completed all prior year recommendations. However, while CNCS had defined a budget for its funding on background investigations, it had not yet committed the necessary funding to complete the investigations. Management expected the funding to be available during FY 2020.

²⁹ The PDRs were based off of the Office of Personnel Management's (OPM) Position Designation Automated Tool (PDAT).

³⁰ Tier 1 is an investigation for positions designated as low-risk, non-sensitive (formerly NACI). Tier 2 is moderate risk (formerly MBI) and Tier 4 is high risk (formerly BI).

³¹ Recommendations 15 and 16, Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service, p. 25, (OIG Report No. 19-03, March 1, 2019).

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FISCAL YEAR 2019 FISMA EVALUATION

In addition, the Contracting Officer's Representative (COR) did not properly monitor their Momentum contractors to ensure they had investigations. As a result, OHC was unaware of the two Momentum contractors and had not conducted an investigation for these contractors. Therefore, we made three new recommendations to address the issue.

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.

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

Recommendation 18: Complete background investigations in accordance with the developed schedule based on prioritization of higher-level risk. (New) (FY19 – FISMA – NFR 5)

Recommendation 19: Develop and implement a written process to ensure that Contracting Officer's Representatives are aware of their roles and responsibilities related to contractor background investigations. The process should require Contracting Officer's Representatives regularly provide the Office of Human Capital a list of names of contractors, who require background investigations, and their associated companies. (New) (FY19 – FISMA – NFR 5)

Recommendation 20: Develop and implement a written process to ensure the Office of Human Capital completes background investigations for all contractors. (New) (FY19 – FISMA – NFR 5)

9. CNCS Must Strengthen Data Protection and Privacy Controls

FY 2019 IG FISMA Metric Area: Data Protection and Privacy

CNCS did not ensure data protection and privacy controls were effectively implemented. According to OMB, protecting an individual's privacy is of utmost importance and an individual's privacy should be considered and protected throughout the information life cycle. As such, organizations are to limit the creation, collection, use, processing, storage, maintenance, dissemination, and disclosure of PII to that which is legally authorized, relevant, and reasonably deemed necessary for the proper performance of Agency functions.³²

Specifically, we noted the following issues:

- Physical access and identification badges (IDs) issued by and utilized for the NCCC Pacific Region campus members contain two artifacts of PII: full name and birthdate. These badges are worn by all NCCC members at the Pacific Region campus for

³² OMB Circular No. A-130, *Managing Information as a Strategic Resource*.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

identification purposes and building access with clear visibility to the public. In addition, the Pacific Region campus utilizes an excess Team Leader laptop for retention of member badges' photographs and the creation of the members' identification cards. The laptop contains a listing of all current Pacific Region campus members and their birthdates. The Team Leader laptop is network capable and generally stored in a locked cabinet when the laptop is not in use. When we inspected the Team Leader laptop, however, it was not current with system patches. OMB Circular A-130, *Managing Information as a Strategic Resource*, July 28, 2016, Appendix 1, requires agencies to implement and maintain current updates and patches for all software and firmware components of information systems.

The NCCC Pacific Region campus management stated the badges were used by members as identification for air travel because many members do not have a government-issued ID card and therefore, the names and birthdates were printed on the badges. In addition, management stated that the campus used an excess Team Leader laptop for member badge creation because the ID installation software is not approved for use on the network and therefore must be used on a non-network machine. However, when we inspected the Team Leader laptop, it was capable of connecting to the Internet.

- The NCCC Southwest Region Campus retained physical counselor files,³³ which include PII and health information of NCCC members, beyond the six-year retention policy. NCCC Southwest Region Campus management stated that the current point of contact for the counselor files did not fully understand the data retention requirements when the campus took ownership of the files following a staff transition.

According to NIST SP 800-53, Revision 4, organizations are to identify and limit the collection of PII that is necessary to accomplish the purpose of collecting the information. Additionally, organizations are to retain each collection of PII for an organization-defined time period.

AmeriCorps NCCC Manual, Section 202, states that member files must be kept at the campus for six years after the date of the member's graduation. Physical member files are shredded.

Without implementing adequate data protection and privacy controls, PII may be mishandled, which could result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII.

To assist CNCS in strengthening data protection and privacy controls, we recommend that CNCS:

Recommendation 21: Assess the NCCC campus member credentialing process and mechanism to ensure compliance with CNCS personnel security policy for badging. (New) (FY19 – FISMA – NFR 4)

Recommendation 22: Document and implement a policy to minimize personally identifiable information on the physical access and identification badges utilized for NCCC Pacific Region Campus members. (New) (FY19 – FISMA – NFR 4)

³³ Class sizes at the NCCC Southwest Region Campus have historically ranged more than 100 members, with one to two classes occurring each year. In order to comply with the data retention and disposal policy, at least two to three classes of files would have needed to be disposed.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Recommendation 23: *Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus. (New) (FY19 – FISMA – NFR 4)*

Recommendation 24: *Periodically provide training for the NCCC campus personnel on the data retention and disposal requirements. (New) (FY19 – FISMA – NFR 4)*

Recommendation 25: *Document and implement a process to validate that physical counselor files from the NCCC Southwest Region Campus are disposed of within six years after the date of the member's graduation in accordance with the AmeriCorps NCCC Manual. (New) (FY19 – FISMA – NFR 4)*

10. CNCS Must Improve Physical Access Controls

FY 2019 IG FISMA Metric Area: Identity and Access Management

CNCS did not ensure physical access controls were effectively implemented to secure certain assets. Physical controls should be in place to protect CNCS facilities and information system assets from unauthorized access.

Specifically, we noted the following issues:

- Packages containing information system assets, including computers, printers, two network switches, an uninterruptible power supply, a copier and printers, which were sent from the Minneapolis, Kansas City, and Denver State Offices (due to state office closures), were left unattended in a publicly-accessible area outside the CNCS HQ mail room. Management stated that the packages regardless of the sensitivity of the content or size, mailed to HQ from State Offices did not require a signature for receipt. Therefore, if the packages were delivered when an attendant was not present at the HQ mailroom, they would be left in a publicly-accessible area outside of the secure mail room. Without properly securing packages, the risk of theft is increased, potentially exposing sensitive data to unauthorized individuals if the package contains IT assets.
- NCCC Southwest Region Campus' networking infrastructure, including its network switches, wireless access controller, and HQ's network switch, was not properly secured by either a locked room or cage at the NCCC Southwest Region Campus, allowing for unrestricted access to the network devices. HQ and NCCC Southwest Region Campus management stated that due to a lack of oversight, the network devices were not properly secured. The lack of secured networking infrastructure at the NCCC Southwest Region Campus increases the risk of unauthorized access to these devices. Network devices are easy targets for malicious attackers to monitor, modify, or deny traffic to and from hosts inside the network. Gaining unauthorized access to the networking infrastructure escalates the risk. In addition, trust relationships can be leveraged to gain access to other hosts on the network. Ultimately, CNCS's information systems could be compromised, leading to unauthorized access and disclosure of sensitive information.

NIST SP 800-53, Revision 4, requires organizations to provide security safeguards to control access to areas within the facility officially designated as publicly accessible.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

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

Recommendation 26: *Develop and implement a written process to ensure all packages with information system assets that are delivered to HQ require a receipt signature. (New) (FY19 – FISMA – NFR 3)*

Recommendation 27: *Develop and implement a written process to ensure all mail, including packages, are securely stored either in the HQ mail room or a secured dropbox. (New) (FY19 – FISMA – NFR 3)*

Recommendation 28: *Secure the networking infrastructure located at the NCCC Southwest Region Campus in a locked room or cage. (New) (FY19 – FISMA – NFR 3)*

**Security Function: Protect
Maturity Model Scoring**

We assessed CNCS’s maturity level for the Protect function as Level 2 (*Defined*). As shown in Table 2, the maturity levels of the four domains in the Protect function scored a four-way tie, with one domain at each level: configuration management at Level 1 (*Ad Hoc*); identity and access management at Level 2; data protection and privacy at Level 3 (*Consistently Implemented*) and security training at Level 4 (*Managed and Measurable*). The metrics’ algorithm defaults to the higher rating in the event of a tie, which rated CNCS as *Managed and Measurable* for the entire Protect function. However, IGs have the discretion to determine the overall effectiveness rating and the rating for each of the Cybersecurity Framework Functions at the maturity level of their choosing and explain the rationale for their effectiveness ratings. Here, we assessed the Protect Function’s maturity level as *Defined* (Level 2), because CNCS’s strong performance with respect to security training is outweighed by the severity of the control weaknesses in the other three domains. These control weaknesses leave CNCS’s systems vulnerable to unauthorized access, loss of personally identifiable information and disruption. Thus, a score of Level 2 accurately reflects the overall maturity of the Protect function at CNCS.

Function	Count	IG FISMA Metric Questions
Ad Hoc (Level 1)	3	16, 17, and 18
Defined (Level 2)	10	15, 19, 23, 24, 25, 26, 27, 28, 29, and 30
Consistently Implemented (Level 3)	5	20*, 21, 33, 35, and 36
Managed and Measurable (Level 4)	9	14**, 31, 34, 37, 39**, 41, 42, 43, and 44
Optimized (Level 5)	1	40
Calculated Maturity Level: Managed and Measurable (Level 4), Effective		
Assessed Maturity Level: Defined (Level 2), Not Effective		

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

** Questions 14 and 39 met the highest maturity level in the reporting metrics of “Managed and Measurable”

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

The FY 2018 FISMA evaluation report³⁴ included a recommendation for CNCS to perform an analysis of the IG FISMA Metrics related to the security function “Protect” and develop a multi-year strategy that addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. At the conclusion of our testing in August 2019, management indicated a date of September 30, 2019, as the date for completion.

In addition, our judgmental assessment is Not Effective for the Protect function, based on the control weaknesses noted during our independent evaluation related to configuration management, identity and access management, and data protection and privacy. Since the prior year recommendation was not completed and multiple control weaknesses were reported in the “Protect” function area, we make the same recommendation this year to assist CNCS in reaching an effective rating for the “Protect” function area. We recommend CNCS:

Recommendation 29: *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. (Repeat)*

³⁴ Recommendation 21, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 27 (OIG Report No. 19-03, March 1, 2019).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

Security Function: Detect

11. CNCS Must Enhance the Review and Analysis of Wireless Network Audit Logs

FY 2019 IG FISMA Metric Area: *Information Security Continuous Monitoring*

NCCC Pacific and Southwest Region campus personnel did not review and analyze wireless network logs for their NCCC members. 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.). They did not review wireless network activities, including who connected to the network, connections made after normal business hours, and how much bandwidth was being used by each client.

The Pacific Region Campus wireless service is provided under an internal OIT contract vehicle, while the Southwest Region Campus wireless service is provided externally on a separate IT contract. The NCCC Southwest Region Campus wireless contract included a service to allow NCCC staff to better manage the wireless network. However, NCCC Southwest Region Campus personnel did not enable the audit logging function on the wireless controller and they also did not monitor the contractor to ensure all logging services were being provided.

When we reviewed the NCCC Pacific Region Campus' wireless network, the campus management and OIT were unsure which wireless network contract was being managed. After an OIT's internal review, it discovered that the NCCC Pacific Region Campus wireless service contract was under an existing OIT contract vehicle. The NCCC Pacific Region Campus personnel were not aware of their responsibilities under the contract to monitor the wireless network activity logs.

After OIT management was notified of the issues at the NCCC Pacific and Southwest campuses, it decided to exert more oversight for both contracts. OIT management stated that an OIT representative was assigned as a subject matter expert and an alternate campus ordering official to the NCCC Southwest wireless contract. The NCCC Pacific Region Campus wireless contract remains under the existing OIT contract vehicle, but the OIT COR will be more involved in vendor management and approving invoices.

NIST requires organizations to review and analyze information system audit records at a defined frequency for indications of inappropriate or unusual activity, and report findings to defined personnel or roles.

Without reviewing the wireless network logs, the Pacific and Southwest Region campus personnel may not maintain an understanding of the active and historic activities occurring from the wireless access points. This significantly reduces the campuses personnel's ability to detect suspicious activity and potentially malicious users, increasing the risk of unauthorized access to sensitive information.

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

Recommendation 30: *Develop and implement a written process to review and analyze the wireless network logs at the NCCC Pacific and Southwest Regional Campuses. (New) (FY19 – FISMA – NFR 10)*

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

**Security Function: Detect
Maturity Model Scoring**

The calculated maturity level based on the five IG FISMA Metric questions for the “Detect” function is Level 1 (*Ad-Hoc*) or 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)	1	48
Consistently Implemented (Level 3)	1	47
Managed and Measurable (Level 4)	1	49
Optimized (Level 5)	0	N/A
Calculated Maturity Level: Ad-Hoc (Level 1), Not Effective		

The FY 2018 FISMA evaluation report³⁵ made a recommendation for CNCS to perform an analysis of the IG FISMA Metrics related to the security function “Detect” and develop a multi-year strategy that addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. At the conclusion of our testing in August 2019, management indicated a date of September 30, 2019, for completion.

Since the prior year recommendation was not completed, we made the same recommendation this year to assist CNCS in reaching an effective rating for the “Detect” function area. We recommend CNCS:

Recommendation 31: 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. (Repeat)

³⁵ Recommendation 23, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 29 (OIG Report No. 19-03, March 1, 2019).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

**Security Function: Respond
Maturity Model Scoring**

Although our judgmental assessment did not find any weaknesses for controls evaluated in the “Respond” function, the calculated maturity level based on the seven IG FISMA Metric questions for the function area is Level 3 (*Consistently Implemented*) or 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)	5	52, 54, 55, 56, and 58
Managed and Measurable (Level 4)	2	53* and 57*
Optimized (Level 5)	0	N/A
Calculated Maturity Level: Consistently Implemented (Level 3), Not Effective		

* Questions 53 and 57 met the highest maturity level in the reporting metrics of “Managed and Measurable”

The FY 2018 FISMA evaluation report³⁶ included a recommendation for CNCS to perform an analysis of the IG FISMA Metrics related to the security function “Respond” and develop a multi-year strategy that addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. At the conclusion of our testing in August 2019, management indicated a date of September 30, 2019, for completion.

Since the prior year recommendation was not completed, we made the same recommendation this year to assist CNCS in reaching an effective rating for the “Respond” function area. We recommend CNCS:

We recommend CNCS:

Recommendation 32: 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. (Repeat)

³⁶ Recommendation 24, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 30 (OIG Report No. 19-03, March 1, 2019).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FISCAL YEAR 2019 FISMA EVALUATION**

**Security Function: Recover
Maturity Model Scoring**

Although our judgmental assessment did not find any weaknesses for controls evaluated in the “Recover” function, the calculated maturity level based on the seven IG FISMA Metric questions for the function area is Level 3 (*Consistently Implemented*) or 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)	4	62*, 64, 65*, and 66
Managed and Measurable (Level 4)	3	60**, 61 and 63
Optimized (Level 5)	0	N/A
Calculated Maturity Level: Consistently Implemented (Level 3), Not Effective		

* Questions 62 and 65 met the highest maturity level in the reporting metrics of “Consistently Implemented”

** Question 60 met the highest maturity level in the reporting metrics of “Managed and Measurable”

The FY 2018 FISMA evaluation report³⁷ made a recommendation for CNCS to perform an analysis of the IG FISMA Metrics related to the security function “Recover” and develop a multi-year strategy that addresses the corrective actions necessary to show steady, measurable improvement towards an effective information security program. At the conclusion of our testing in August 2019, management indicated a date of September 30, 2019, for completion.

Since the prior year recommendation was not completed, we made the same recommendation this year to assist CNCS in reaching an effective rating for the “Recover” function area. We recommend CNCS:

We recommend CNCS:

Recommendation 33: 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. (Repeat)

³⁷ Recommendation 25, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 31 (OIG Report No. 19-03, March 1, 2019).

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix I

BACKGROUND

CNCS 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. CNCS relies on IT systems to accomplish its mission of making grants and managing a residential national service program. CNCS has a FISMA inventory of six information systems – the Network or GSS, eSPAN (which includes the eGrants grants management system), Momentum Financial Management System (Momentum), AmeriCorps Health Benefits, AmeriCorps Childcare Benefits System, and public websites.³⁸ The first five of these systems are categorized as moderate security, while the public websites are rated as low security.³⁹ All six systems are hosted and operated by third-party service providers, although CNCS hosts certain components of the GSS. CNCS's network consists of multiple sites: HQ, one Field Financial Management Center (FFMC), and four NCCC campuses. These facilities are connected through commercially managed telecommunications network connections.

Beginning in May 2019, CNCS began the closure of 43 AmeriCorps State Offices. The closure occurred in three phases between May, June, and July. CNCS has continued operations remotely for each office closure and has plans to create eight Regional Offices beginning in October.

To balance high levels of service and reduce costs, CNCS's OIT has outsourced the operation, maintenance, and support of most of CNCS's IT systems. Despite this, CNCS by law retains responsibility for complying with the requirements of the FISMA and security control implementation.

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 the 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

³⁸ 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.

³⁹ 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.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix I

needed to produce and provide financial reports and internal controls. Momentum is housed in Chantilly, Virginia. CNCS is in the process of implementing PRISM for procurement activities. PRISM was scheduled to go live on October 1, 2019. PRISM, during its Phase 1 of implementation, was utilized to initiate procurement activities, which were then manually entered into Momentum Acquisitions. At the conclusion of our testing in August 2019, Phase 2 of implementation, which automates the interface between PRISM and Momentum Acquisitions, was scheduled for October 1, 2019.

- **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 grant-making: applying, awarding, monitoring, reporting, and closeout. eGrants also interfaces with Momentum and, through Momentum, with the Department of Health and Human Services' Payment Management System.

CNCS OIT provides support for CNCS's technology and information needs, as well as project management services during the life cycle of major system acquisitions through daily operations. The Chief Information Officer (CIO) leads the OIT and CNCS's IT operations. The CIO is assisted by the CISO, who manages the OIT/Cybersecurity office responsible for computer security and privacy issues and addressing the 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 NIST SP 800-53, Revision 4.

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 OMB and to congressional committees on the effectiveness of their information security program.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix I

Federal agencies are to provide information security protections commensurate to 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 the Agency’s IGs to assess the effectiveness of agency information security programs and practices. Guidance has been issued by OMB and by NIST (in its 800 series of Special Publications) supporting FISMA implementation. In addition, NIST issued the Federal Information Processing Standards (FIPS) to establish Agency baseline security requirements.

FY 2019 IG FISMA Reporting Metrics

OMB and Department of Homeland Security (DHS) annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On October 25, 2018, OMB issued Memorandum M-19-02, *Fiscal Year 2018-2019 Guidance on Federal Information Security and Privacy Management Requirements*. This memorandum describes the processes for federal agencies to report to OMB and, where applicable, DHS. Accordingly, the *FY 2019 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics*, provided reporting requirements across key areas to be addressed in the independent assessment of agencies’ information security programs.⁴⁰

The FY 2019 IG FISMA Reporting Metrics (IG FISMA Metrics) incorporates a maturity model that aligns with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1 Identify, Protect, Detect, Respond and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity 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 4**.

Table 4: Aligning the NIST Cybersecurity Framework Security Functions to the FY 2019 IG FISMA Metric Domains

NIST Cybersecurity Framework Security Functions	FY 2019 IG FISMA Metrics Domains
Identify	Risk Management
Protect	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Information Security Continuous Monitoring
Respond	Incident Response
Recover	Contingency Planning

⁴⁰ <https://www.dhs.gov/publication/fy19-fisma-documents>

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix I

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 5** 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 5: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1 (<i>Ad Hoc</i>)	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2 (<i>Defined</i>)	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Level 3 (<i>Consistently Implemented</i>)	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4 (<i>Managed and Measurable</i>)	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 (<i>Optimized</i>)	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.

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.⁴¹ 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 (two NCCC campuses). The enterprise-level assessment was conducted at the CNCS HQ in Washington, D.C., from March 19, 2019 to August 30, 2019. The facility-level assessment included on-site security assessments at the NCCC Southwest Campus, Denver, Colorado from May 13 to 14, 2019, and NCCC Pacific Campus and Computer Lab, Sacramento, California from May 15 to 16, 2019 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

A network vulnerability assessment was also conducted at the HQ and the NCCC Southwest and Pacific campuses.

⁴¹ <https://www.ignet.gov/sites/default/files/files/committees/inspect-eval/iestds12r.pdf>

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix II

In addition, the evaluation included an assessment of effectiveness for each of the eight FY 2019 IG FISMA Metrics Domains and the maturity level of the five Cybersecurity Framework Security Functions. 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.⁴²

Methodology

Following the framework for minimum security controls in NIST SP 800-53, Revision 4, certain controls were selected from the NIST security control families associated with the FY 2019 IG FISMA Metrics Domains aligned with the Cybersecurity Framework Security Functions.⁴³ **Table 6** lists the selected controls for the four CNCS systems that were reviewed for this evaluation:

Table 6: List of Selected Controls Reviewed

Security Control Family	NIST 800-53 Associated Control ⁴⁴
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-3, SA-4, 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.

⁴² *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 19-03, March 1, 2019).

⁴³ Security controls are organized into families according to their security function—for example, access controls.

⁴⁴ These associated controls are from NIST 880-53, Revision 4, located at <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf>

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix II

- Tested system processes to determine the adequacy and effectiveness of selected controls.
- Performed site visits to determine if controls are consistently implemented across CNCS at the facility level.
- Reviewed the status of recommendations in the FY 2018 FISMA report, including supporting documentation, to ascertain whether the actions taken addressed the weakness.⁴⁵

We exercised professional judgment in determining the number of items selected for testing the adequacy and effectiveness of the security controls and the method used to select sample items. Relative risk and the significance or criticality of the specific control activities or sample items in achieving the related control objectives were considered. In addition, the severity of a deficiency related to the control activity, as opposed to 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 for testing. However, in cases where the entire audit population was not selected, the results cannot be projected and, if projected, the results may be misleading.

⁴⁵ Ibid. footnote 41.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

STATUS OF PRIOR YEAR RECOMMENDATIONS

The following tables summarize our follow up related to the status of open prior-year recommendations reported in the FY 2014, 2016, 2017 and 2018 FISMA evaluations.^{46 47 48 49} There were no open recommendations from the FY 2015 FISMA evaluation.

During FY 2019, CNCS implemented corrective actions to close 21 prior year recommendations from the FY 2014, 2016, 2017, and 2018 FISMA evaluations.

Status of Prior Year FY 2014 Recommendations

FISMA NFRs	FY 2014 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY14 – FISMA – NFR 9	Recommendation 1: Document and fully implement a comprehensive and enterprise-wide risk management process, including the following:		
	<i>Part B:</i> 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.	Closed	Remains Open Modified Repeat, refer to Finding 3
	<i>Part C:</i> 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.	Closed	Remains Open Modified Repeat, refer to Finding 3

⁴⁶ *The Federal Information Security Management Act, Fiscal Year 2014, evaluation of the Corporation for National & Community Service* (OIG Report No. 15-03, November 14, 2014).

⁴⁷ *Fiscal Year 2016 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 17-03, December 21, 2016).

⁴⁸ *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).

⁴⁹ Ibid. footnote 41.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

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	<p>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.</p>	Open	Remains Open Modified Repeat, refer to Finding 4
	<p>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.</p>	Open	Remains Open Modified Repeat, refer to Finding 4
	<p>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.</p>	Open	Remains Open Modified Repeat, refer to Finding 4

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

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	<p>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.</p>	Closed	Closed
	<p>Recommendation 4: Document and implement a process to assess and acknowledge the information security and privacy risks to the Corporation associated with the use of all external information systems. This can include reviews of the Service Organization Control reports or risk assessments performed for external systems to gain an understanding of the information security risks identified, and assess and document the risks to CNCS from the use of these systems.</p>	Closed	Closed
FY17-FISMA-NFR 8	<p>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:</p> <ul style="list-style-type: none"> • Finalizing the risk register • Establishing the risk tolerance for the Corporation, including information security and privacy, and communicating the risk tolerance throughout the organization 	Closed	Remains Open Modified Repeat, refer to Finding 3

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	<ul style="list-style-type: none"> Developing, documenting, and implementing acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance Developing, documenting, and implementing approaches for monitoring risk over time 		
FY17-FISMA-NFR 5	<p>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.</p>	Open	Remains Open Modified Repeat, refer to Finding 4
	<p>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.</p>	Open	We noted no exceptions in our testing of a sample of system changes this year. Closed
FY17-FISMA-NFR 9	<p>Recommendation 14: Implement PIV multifactor authentication for local and network access for privileged users.</p>	Open	Remains Open Modified Repeat, refer to Finding 5
	<p>Recommendation 15: Implement PIV multifactor authentication for network access for non-privileged users.</p>	Open	Remains Open Modified Repeat, refer to Finding 5
FY17-FISMA-NFR 7	<p>Recommendation 16: Complete the process for aggregating the Momentum Oracle</p>	Closed	Closed

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	database security logs into the Splunk tool.		
FY17-FISMA-NFR 4	<p>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.</p>	Closed	Closed
FY17-FISMA-NFR 1	<p>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:</p> <ul style="list-style-type: none"> • 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	Remains Open Modified Repeat, refer to Finding 1
	<p>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.</p>	Open	Remains Open 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

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
			those sites. Management stated that corrective action was not completed.
	<p>Recommendation 26: Ensure the facilities implement the following in regard to protection of mobile devices:</p> <ul style="list-style-type: none"> • 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	<p align="center">Remains Open</p> <p>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.</p>
	<p>Recommendation 27: Ensure the facilities implement the following in regards to protection of mobile devices:</p> <ul style="list-style-type: none"> • 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	<p align="center">Remains Open</p> <p>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.</p>
	<p>Recommendation 28: Ensure the Vicksburg NCCC campus implements the following regarding the OpenDNS service:</p>	Closed	Closed

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	<ul style="list-style-type: none"> • Remove the unnecessary account to the OpenDNS service, and create a new account for administrative access. • Review the OpenDNS reports for the wireless network. 		
	<p>Recommendation 29: Configure CNCS issued laptops to deny the use of the FEMA wireless network by service set identifier (SSID).</p>	Closed	<p align="center">Remains Open</p> <p>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 "Access to the FEMA Wireless network is required by users and necessary for their job functions. It cannot be denied." Management had not completed Risk Acceptance.</p>
	<p>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.</p>	Closed	Closed
	<p>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.</p>	Closed	Closed

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

Status of Prior Year FY 2018 Recommendations

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY18 – FISMA – NFR 6	<p>Recommendation 1: Ensure that OIT monitor and promptly install patches and antivirus updates across the enterprise when they are available from the vendor. Enhancements should include:</p>		
	<p><i>Part A:</i> Implement a process to track patching of network devices and servers by the defined risk-based patch timelines in CNCS policy.</p>	Open	Remains Open Modified Repeat, refer to Finding 1
	<p><i>Part B:</i> Ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer.</p>	Open	Remains Open Modified Repeat, refer to Finding 1
	<p><i>Part C:</i> 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.</p>	Open	Remains Open Modified Repeat, refer to Finding 1
	<p><i>Part D:</i> Enhance the inventory process to ensure all devices are properly identified and monitored.</p>	Open	Remains Open Modified Repeat, refer to Finding 2
	<p>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.</p>	Open	Remains Open 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.
FY18-FISMA-NFR 1	<p>Recommendation 3: Ensure the Chief Information Security Officer validates the security</p>	Closed	Closed

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	authorization process is maintained in accordance with OMB and NIST requirements.		
FY18-FISMA-NFR 9	Recommendation 4: Develop and document a comprehensive risk register at the mission and business process level.	Open	Remains Open Modified Repeat, refer to Finding 3
FY18-FISMA-NFR 3	Recommendation 5: Ensure the system risk assessments include all NIST required risk assessment elements, including the missing elements of likelihood and impact analysis.	Closed	Closed
FY18-FISMA-NFR 7	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.	Closed	Closed
FISMA Metrics	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.	Open	Remains Open
FY18-FISMA-NFR 10	Recommendation 8: Ensure that standard baseline configurations for all platforms in the CNCS information technology	Open	Remains Open Modified Repeat, refer to Finding 4

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	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.		
	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.	Closed	Closed
	Recommendation 10: Implement a process to ensure that functional testing occurred, and documentation is maintained for system changes.	Open	We noted no exceptions in our testing of a sample of system changes this year. Closed
FY18-FISMA-NFR 4	Recommendation 11: Implement Personal Identification Verification multifactor authentication for local and network access for privileged users.	Open	Remains Open Modified Repeat, refer to Finding 5
	Recommendation 12: Implement Personal Identification Verification multifactor authentication for network access for non-privileged users.	Open	Remains Open Modified Repeat, refer to Finding 5
FY18-FISMA-NFR 11	Recommendation 13: Ensure disabled network accounts for separated individuals are removed from the Active Directory Subversion Organizational Unit.	Closed	Closed
	Recommendation 14: Ensure that periodic reviews are conducted of user accounts with access to the Subversion OU within Active Directory.	Closed	Closed
FY18-FISMA-NFR 2	Recommendation 15: Perform and document an assessment of staffing and funding	Closed	Closed

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
	levels required for background investigations and address any recognized gaps.		
	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.	Closed	Closed
FY18-FISMA-NFR 5	Recommendation 17: Require FFMC to implement corrective actions to secure the facility with doors that do not pose a security risk to the facility.	Closed	Closed
	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.	Closed	Closed
	Recommendation 19: Require Vinton NCCC campus to implement corrective actions to ensure the camera feeds are monitored.	Closed	Closed
	Recommendation 20: Require FFMC and the Vinton NCCC campus to conduct and document a physical security risk assessment.	Open	Remains Open
FISMA Metric	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.	Open	Remains Open

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status Determined by CNCS
FY18-FISMA-NFR 8	Recommendation 22: Complete the process for aggregating the Momentum Oracle database security logs into the security event management system (i.e., Splunk tool).	Closed	Closed
FISMA Metric	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.	Open	Remains Open
FISMA Metric	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.	Open	Remains Open
FISMA Metric	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.	Open	Remains Open



CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION

Appendix IV

MANAGEMENT COMMENTS



To: Monique Colter, Assistant Inspector General for Audit

From: Pape Cisse, Chief Information Officer (CIO)  Pape Cisse
Andrea Simpson, Chief Information Security Officer (CISO)  ANDREA SIMPSON

Cc: Lisa Guccione, Chief of Staff
Tim Noelker, General Counsel

Date: December 30, 2019

Subject: Management's Response to Office of Inspector General's Draft Report: Fiscal Year 2019 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 (FY) 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service.

The draft report highlights a recommendation that CNCS complete a strategic analysis of the government-wide metrics and the weaknesses identified in the evaluation and develop a multi-year approach designed to realize steady, measurable improvements in information security in each of the domains and security function areas. CNCS's Office of Information Technology (OIT) has completed an initial analysis for the areas of "Identify" and "Protect," and is scheduled to complete its reviews of the "Detect," "Respond" and "Recover" areas in the near future. Once these initial analyses are complete, CNCS will review the steps needed to respond to the identified needs. Development of a final approach will also depend upon the resources available for CNCS to address its information security needs.

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

Security Function: Identify

1. CNCS must improve its Vulnerability and Patch Management Controls

CNCS Response: CNCS concurs that unpatched software and improper configuration settings exposes the CNCS network to preventable vulnerabilities. However, there are many mitigating factors in place that reduce the risk of those vulnerabilities being exploited.

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.
- Replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer.

250 E Street, SW
Washington, D.C. 20525
202-606-5000 | 800-942-2677 | TTY 800-833-3722



**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix IV

- 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.
- Enhance the inventory process to ensure all devices are properly identified and monitored.

CNCS Response: As part of the Enterprise Information Technology Service (eITS) contract award, CNCS will ensure that specific service level agreements (SLAs) will make the service provider responsible for maintaining a secure network in accordance with OIT policies and procedures. The SLAs will address the first three items of the recommendation. The last item regards how CNCS conducts inventory. The CNCS system of record for IT equipment is Remedy Force. Historically, IT purchases by NCCC have not been included in CNCS's inventory. To better manage CNCS's full IT asset inventory, OIT has engaged with NCCC to determine how best to address the issue of maintaining a complete IT inventory.

Recommendation 2: Ensure that OIT evaluates if the internet connections at the National Civilian Community Corps Campuses and Regional 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.

CNCS Response: The Enterprise Infrastructure Solutions (EIS) contract will be awarded in FY20. The internet connections to existing and planned offices will be optimized upon award execution.

Recommendation 3: Create accounts for CNCS OIT's Infrastructure staff identified by the Director of Infrastructure for monitoring the vulnerability scanning tool and validating vulnerability management activities on the networks and devices they manage.

CNCS Response: CNCS concurs and will implement this recommendation before the end of the second quarter of Fiscal Year 2020.

2. CNCS Must Improve its Inventory Management Process

CNCS Response: CNCS concurs that it needs a reliable Inventory Management Process.

Recommendation 4: Develop and implement a written process to ensure manual updates to the CMDB inventory and FasseTrack system are made simultaneously when the inventory is updated.

CNCS Response: CNCS concurs. CNCS will develop processes to ensure that the CNCS inventory system of record is accurate. As noted in response to Recommendation 7, CNCS intends to automate the inventory process as much as possible. The development of specific written procedures to supplement that process should await the results of the automation.

Recommendation 5: Develop and implement a written process to ensure Remedy Force tickets are completed at the time the inventory is updated.

CNCS Response: CNCS concurs. However, as noted in response to Recommendation 7, CNCS intends to automate the inventory process as much as possible. The development of specific written procedures to supplement that process should await the results of the automation.

Recommendation 6: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FY 2019 FISMA EVALUATION

Appendix IV

CNCS Response: CNCS concurs. However, as noted in response to Recommendation 7, CNCS intends to automate the inventory process as much as possible. The development of specific written procedures to supplement that process should await the results of the automation.

Recommendation 7: Perform and document analysis to determine the feasibility of completely automating the inventory management process.

CNCS Response: CNCS concurs. CNCS has budgeted to upgrade existing inventory tools that will automate inventory as much as possible. In addition, by the end of Fiscal Year 2020 CNCS will have DHS, Continuous Diagnostic and Mitigations (CDM) capability fully implemented which has a hardware and software inventory component.

3. CNCS Must Fully Implement its Organization-wide Risk Management Program

FY 2019 IG FISMA Metric Area: *Risk Management*

CNCS Response: 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.

Recommendation 8: Continue the current effort to complete a comprehensive risk register at the mission and business process level.

CNCS Response: CNCS partially concurs with this response. CNCS has an Enterprise Risk Register, which 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. CNCS plans to update and continue the development of its mission and business process level risk registry.

Recommendation 9: 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.

CNCS Response: CNCS concurs. A high-level plan has been developed that lays out a clear path for CNCS to improve targeted areas related to the “Identify” security function.

4. CNCS Must Implement Standard Baseline Configurations

FY 2019 IG FISMA Metric Area: *Configuration Management*

CNCS Response: CNCS concurs that a baseline configuration will provide a repeatable process to ensure that devices are established at a high level of efficiency and security.

Recommendation 10: Establish and document standard baseline configurations for all platforms in the CNCS information technology environment and ensure these standard baseline configurations 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.

CNCS Response: CNCS concurs. CNCS will create guidance on how to create a configuration baseline that meets CNCS security requirements, which will include the approval process. Information System

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix IV

Security Officers (ISSOs) will incorporate the guidance into the configuration and system security plans (SSPs) for their respective systems in order to maintain their ongoing authorization.

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

FY 2019 IG FISMA Metric Area: Identity and Access

CNCS Response: CNCS concurs and has started the process of implementing multifactor authentication.

Recommendation 11: Implement Personal Identification Verification multifactor authentication for local and network access for privileged users to all workstations and servers.

CNCS Response: CNCS concurs with this finding. CNCS will complete its multifactor authentication implementation in FY20.

Recommendation 12: Complete the implementation of Personal Identification Verification multifactor authentication for network access for all non-privileged users by upgrading all users to Microsoft Windows 10 workstations and enforcing logon with a Personal Identification Verification card.

CNCS Response: CNCS concurs with this finding and is on track to complete the task before the end of FY20.

6. CNCS Must Strengthen Account Management Controls

FY 2019 IG FISMA Metric Area: Identity and Access Management

CNCS Response: CNCS concurs that it needs to improve the account management process used by its primary information systems.

Recommendation 13: Develop and implement a written process for the Director of Infrastructure to monitor the employee separation process to ensure CNCS policy is followed for disabling system accounts within one working day following separated employees' termination and disabled network accounts of separated individuals are removed from the Active Directory My AmeriCorps Staff Portal Organizational Unit.

CNCS Response: CNCS concurs and has started to create a process to ensure internal and external accounts are disabled according to policy.

Recommendation 14: Enhance information systems to automatically disable user accounts after 30 days of inactivity in accordance with CNCS policy. This includes monitoring automated scripts to validate accounts are disabled properly.

CNCS Response: CNCS concurs and has started to create a process to ensure internal and external accounts are disabled according to policy.

Recommendation 15: Develop and implement a written process for the Chief Information Security Officer to ensure an account quarterly review/recertification is performed for Momentum.

CNCS Response: CNCS does not concur with recommendation and will take no further action. A process currently exists as part of the continuous monitoring process to validate that account recertification occurs. Each missed occurrence is documented and reported to the Authorizing Official. In addition, CNCS is in the process of migrating its accounting systems to a shared services provider,

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix IV

and therefore the risks that would be mitigated by this recommendation we anticipate to be eliminated by the end of Fiscal Year 2020.

Recommendation 16: Develop and Implement a written process that ensures all CNCS information system passwords are changed at the frequency specified in applicable CNCS policy or the System Security Plan.

CNCS Response: CNCS concurs and is exploring multiple options that will either improve password management or move to multifactor or third-party authentication methods.

7. CNCS Must Ensure All Information System Users Complete Access Agreements

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

CNCS Response: CNCS concurs, however by policy all users must acknowledge the CNCS Rules of Behavior (ROB) in the first quarter of the fiscal year.

Recommendation 17: Develop and implement a written process for the Information Security Officer to validate that all new information system users complete the Rules of Behavior prior to gaining system access in accordance with CNCS policy.

CNCS Response: CNCS will develop a process prior to the start of the fiscal year to validate new users have acknowledged the ROB.

8. CNCS Must Enhance the Personnel Screening Process

FY 2019 IG FISMA Metric Area: *Identity and Access Management*

CNCS Response: CNCS concurs and is continuing to improve the personnel screening process.

Recommendation 18: Complete background investigations in accordance with the developed schedule based on prioritization of higher-level risk.

CNCS Response: CNCS concurs that anyone, employee or contractor, who has access to valuable CNCS information should 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. CNCS will continue to execute its current plan to completion.

Recommendation 19: Develop and implement a written process to ensure that Contracting Officer's Representatives are aware of their roles and responsibilities related to contractor background investigations. The process should require Contracting Officer's Representatives regularly provide the Office of Human Capital a list of names of contractors who require background investigations and their associated companies.

CNCS Response: CNCS concurs and will review the recommended process to determine its feasibility in current and future plans.

Recommendation 20: Develop and implement a written process to ensure the Office of Human Capital completes background investigations for all contractors.

CNCS Response: CNCS concurs and will review the recommended process to determine its feasibility in current and future plans.

9. CNCS Must Strengthen Data Protection and Privacy Controls

CORPORATION FOR NATIONAL AND COMMUNITY SERVICE FY 2019 FISMA EVALUATION

Appendix IV

FY 2019 IG FISMA Metric Area: Data Protection and Privacy

CNCS Response: CNCS concurs that protection of CNCS information is essential in providing services to CNCS employees and members.

Recommendation 21: Assess the NCCC campus member credentialing process and mechanism to ensure compliance with CNCS personnel security policy for badging.

CNCS Response: CNCS concurs and will issue guidance on baseline badging requirements.

Recommendation 22: Document and implement a policy to minimize personally identifiable information on the physical access and identification badges utilized for NCCC Pacific Region Campus members.

CNCS Response: CNCS concurs and will issue guidance on baseline badging requirements.

Recommendation 23: Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.

CNCS Response: CNCS concurs and will disable network capability.

Recommendation 24: Periodically provide training for the NCCC campus personnel on the data retention and disposal requirements.

CNCS Response: CNCS concurs and will maintain alignment with current CNCS records management training requirements.

Recommendation 25: Document and implement a process to validate that physical counselor files from the NCCC Southwest Region Campus are disposed of within six years after the date of the member's graduation in accordance with the AmeriCorps NCCC Manual.

CNCS Response: CNCS will issue guidance to dispose of all physical counselor files at all NCCC campus locations as they are working documents only and are not governed by NCCC records retention policy.

10. CNCS Must Improve Physical Access Controls

FY 2019 IG FISMA Metric Area: Identity and Access Management

CNCS Response: CNCS concurs its physical access controls need to be reviewed and improved to address resource limitations.

Recommendation 26: Develop and implement a written process to ensure all packages with information system assets that are delivered to HQ require a receipt signature.

CNCS Response: CNCS concurs and will develop processes to require that known deliveries of information system assets that may contain personally identifiable information require signature for delivery.

Recommendation 27: Develop and implement a written process to ensure all mail, including packages, are securely stored either in the HQ mail room or a secured dropbox.

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix IV

CNCS Response: CNCS concurs and, if resources allow, will provide a secure dropbox for the delivery of correspondence and packages when the HQ mailroom is unattended.

Recommendation 28: Secure the networking infrastructure located at the NCCC Southwest Region Campus in a locked room or cage.

CNCS Response: CNCS concurs and will identify a locked area or secure the current location.

Security Function: Protect

Recommendation 29: 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.

CNCS Response: CNCS concurs. A high-level plan has been developed that layouts a clear path for CNCS to improve targeted areas related to the “Protect” security function.

11. CNCS Must Enhance the Review and Analysis of Wireless Network Audit Logs

FY 2019 IG FISMA Metric Area: Information Security Continuous Monitoring

CNCS Response: CNCS concurs and will develop a process to address how wireless network access is managed across the enterprise.

Recommendation 30: Develop and implement a written process to review and analyze the wireless network logs at the NCCC Pacific and Southwest Regional Campuses.

CNCS Response: CNCS concurs and has implemented a written process that ensures wireless network logs are available and regularly reviewed at all NCCC campuses.

Security Function: Detect

Recommendation 31: 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.

CNCS Response: CNCS concurs. A high-level plan to improve targeted areas related to the “Detect” security function has been started with an expected completion date in early calendar year 2020.

Security Function: Respond

Recommendation 32: 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.

CNCS Response: CNCS concurs and is planning to have a high-level plan for the “Respond” security function area in early calendar year 2020.

Security Function: Recover

**CORPORATION FOR NATIONAL AND COMMUNITY SERVICE
FY 2019 FISMA EVALUATION**

Appendix IV

Recommendation 33: 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.

CNCS Response: CNCS concurs and is planning to have a high-level plan for the “Recover” security function area in early calendar year 2020.

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@CNCISOIG.GOV | WWW.CNCISOIG.GOV