CORPORATION FOR NATIONAL & COMMUNITY SERVICE

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2020 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF THE CORPORATION FOR NATIONAL AND COMMUNITY SERVICE

OIG Report EV-21-03

Prepared by:

Office of Inspector General

250 E Street, SW

Washington, DC 20525

(202) 606-9390

This report was issued to Corporation management on December 18, 2020. Under the laws and regulations governing audit follow up, the Corporation is to complete its corrective actions by December 18, 2021. Consequently, the reported findings do not necessarily represent the final resolution of the issues presented.

OFFICE OF INSPECTOR GENERAL

CORPORATION FOR
NATIONAL & COMMUNITY SERVICE

December 18, 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 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service (OIG Report EV-21-03)

Enclosed is the final report on the *Fiscal Year 2020 Federal Information Security Modernization Act (FISMA) Evaluation of the Corporation for National and Community Service,* the Office of Inspector General's (OIG) Report EV-21-03. 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.

Our auditors will evaluate Management's corrective actions to the findings and new, modified, and prior year open recommendations during the FY 2021 FISMA evaluation, which will commence in the fourth quarter of FY 2021.

Should you have any questions about this report, please contact me at (202) 875-9360.

Enclosure:
As stated

cc: Lisa Guccione, Chief of Staff
Scott Hefter, Chief Operating Officer
Helen Serassio, General Counsel
Terrence King, Acting Chief Information Security Officer
Jill Graham, Acting Chief Risk Officer
Malena Brookshire, 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 2020

December 17, 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

December 17, 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 (CNCS), Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the FISMA evaluation of CNCS for Fiscal Year (FY) 2020. 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 Inspector General (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. A rating of Level 4 (Managed and Measurable) in a Function Area or Metric Domain is considered effective.

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 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 from prior years. Since FY 2019, CNCS advanced in one of the domains and remained at the same maturity level for the other seven domains. CNCS remained at the same maturity level for the five 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 risk management, configuration management, identity and access management, data protection and privacy, and logging and monitoring practices designed to protect mission-critical systems.

The control weaknesses that have consistently contributed to a lack of advancement in maturity levels for the DHS IG Metrics are: 1) completion of the mission and business process level risk register in order to fully implement the Corporation's risk management strategy; 2) implementation of standard baseline configurations; 3) fully implementing Personal Identify Verification (PIV) multifactor authentication, and 4) vulnerability and patch management.

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, including critical management servers. The overall deployment of vendor patches and system upgrades to mitigate the vulnerabilities was found to be inconsistent and not effective for the CNCS network.

In addition, although CNCS defined the standard baseline configurations to be implemented for the Corporation's information technology assets, the standard baseline configurations were not fully implemented. Information technology components that do not comply with standard baseline configurations increase the risk of a security vulnerability being exploited.

Furthermore, CNCS has not fully implemented multifactor authentication (use of a Personal Identification Verification (PIV) card along with a personal identification number) for all information system users and administrators. Management did not prioritize the implementation of multifactor authentication for privileged users as directed by OMB. Additionally, CNCS removed mandatory enforcement of PIV authentication in March 2020 as a way for facilitating remote access during the COVID-19 pandemic. In response to increased risks with the large number of federal personnel teleworking due to the pandemic, the Cybersecurity and Infrastructure Security Agency issued an alert on March 13, 2020, that recommended among other things, requiring multifactor authentication for all users. 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 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

TABLE OF CONTENTS

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 (IG) to assess annually the effectiveness of the information security program at that IG's agency. The Corporation for National and Community Service (CNCS),[2] Office of Inspector General (OIG) contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the FISMA evaluation for Fiscal Year (FY) 2020. 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;[3] and (2) our judgmental assessment of the information security and privacy program, practices and controls for select systems in the 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*.[4]

Overall, CNCS has made little progress in maturing its information security program since FYs 2018 and 2019. See Tables 1 and 2 below, comparing CNCS's FY 2020 maturity scores by security function and by domain with those of FY 2019 and FY 2018. Most of the maturity metrics for the eight domains and five security functions remain unchanged from prior years. Specifically, since FY 2019, CNCS advanced in only one of the domains, Configuration Management, remaining at the same level in the other seven domains and all five function areas.

[1] The FISMA of 2014 (Public Law 113–283—December 18, 2014).
[2] CNCS began doing business as AmeriCorps on October 1, 2020. For this report purpose, we will continue to use CNCS.
[3] The FY 2020 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.
[4] Ibid 3.

Table 1: Comparison of Maturity Ratings in FY 2018, FY 2019, and FY 2020 by Function

Security Function[5]	Maturity Level by Function FY 2018	Maturity Level by Function FY 2019	Maturity Level by Function FY 2020
Identify	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Protect	Defined[6] (Level 2)	Managed and Measurable[7] (Level 4) – *Calculated rating, Reduced to* Defined (Level 2) – *Assessed rating*	Defined[8] (Level 2)
Detect	Defined (Level 2)	Ad Hoc (Level 1)	Ad Hoc (Level 1)
Respond	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Overall	**Not Effective**	**Not Effective**	**Not Effective**

Table 2: Comparison of Maturity Ratings in FY 2018, FY 2019, and FY 2020 by Domain

Security Function[9]	IG FISMA Metric Domains	Maturity Level by Domain FY 2018	Maturity Level by Domain FY 2019	Maturity Level by Domain FY 2020
Identify	**Risk Management**	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Protect	**Configuration Management**	Defined (Level 2)	Ad Hoc (Level 1)	Defined (Level 2)
	Identity and Access Management	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
	Data Protection and Privacy	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
	Security Training	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)	Managed and Measurable (Level 4)

[5] See Appendix I Table 4 and Table 5 for definitions and explanations of the Cybersecurity Framework Security Functions and Metric Domains.
[6] The most frequent maturity level rating across the Protect CSF function served as the overall scoring.
[7] 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 was outweighed by the severity of the control weaknesses in the other three domains: configuration management, identity and access management, and data protection and privacy.
[8] The most frequent maturity level rating across the Protect CSF function served as the overall scoring.
[9] Ibid 3.

Security Function[9]	IG FISMA Metric Domains	Maturity Level by Domain FY 2018	Maturity Level by Domain FY 2019	Maturity Level by Domain FY 2020
Detect	**Information Security Continuous Monitoring**	Defined (Level 2)	Ad Hoc (Level 1)	Ad Hoc (Level 1)
Respond	**Incident Response**	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)
Recover	**Contingency Planning**	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)	Consistently Implemented (Level 3)

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 500 critical vulnerabilities and more than 1,300 high-risk vulnerabilities in the network, arising from unpatched software, improper configuration settings, and unsupported software, all of which were publicly known prior to 2019. CNCS did not resolve critical vulnerabilities within seven days of occurrence and high-risk vulnerabilities within 30 days as required by its internal operating policies. There are continuing deficiencies related to organization-wide risk management, Information Technology (IT) asset inventory management, configuration management, identity and access management, mobile device 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.

The control weaknesses that have consistently contributed to a lack of advancement in maturity levels for the DHS IG metrics are related to:

- Organization-wide risk management strategy,
- Standard baseline configurations,
- Personal Identify Verification (PIV) multifactor authentication, and
- Vulnerability and patch management program.

These control weaknesses directly affected the maturity levels of individual components of information security as follows:

1. The **Identify** function remained at the *Defined* maturity level this year because the organization-wide risk management strategy was not fully implemented. Specifically, the risk register developed to record identified risks at the mission and business process level, or Tier 2 as defined by the NIST, was outdated and therefore did not reflect risks of the current environment. CNCS management attributed the delay in updating the risk register to shifting resources in response to the COVID-19 pandemic. This control weakness affected four of the 12 metric

questions in the risk management domain. Completing the updated Tier 2 risk register will assist CNCS in increasing the Identify function above the *Defined* maturity level.

2. The **Protect** function also remained at the *Defined* maturity level this year because of the issues related to standard baseline configurations and PIV multifactor authentication. The maturity level of one domain in this function area, configuration management, improved from *Ad Hoc* to *Defined* this year because CNCS defined the standard baseline configurations to be implemented for the Corporation's information technology assets. The domain did not achieve greater maturity because those configurations were not fully implemented, affecting four of the eight metric questions related to configuration management. In addition, the maturity level for the identity and access management domain remained at the *Defined* maturity level because PIV multifactor authentication was still not fully implemented for privileged and non-privileged users. This control weakness affected five of the nine metric questions in this domain. By fully implementing standard baseline configurations and PIV multifactor authentication, CNCS can improve the maturity level of the Protect function above the *Defined* maturity level.

3. The **Detect** function area remains at *Ad Hoc* because CNCS did not consistently remediate vulnerabilities on the schedule required by its *Cybersecurity Information Security Continuous Monitoring Strategy (ISCM)*. In addition, the lack of a Tier 2 risk register inhibits the ability of CNCS to correlate considerations at the organization/business process level in the ISCM Strategy. Finally, CNCS has not identified and defined performance measures for assessing the effectiveness of the ISCM program. These control weaknesses affected four of the five metric questions in the continuous monitoring domain.

Focusing on these controls is key to CNCS increasing the Identify, Protect, and Detect function areas to an effective maturity level.

In addition, CNCS has not made significant progress in closing prior recommendations. Since last year, the agency demonstrated actions to close eleven of the 58 open recommendations from the FY 2014 – FY 2019 FISMA evaluations, yielding slight improvements in IG FISMA metrics results.[10] For example, CNCS documented standard baseline configurations; ensured system users acknowledged access agreements/rules of behavior prior to gaining system access; and ensured quarterly account reviews and recertifications for Momentum.[11] See **Appendix III** for the status of prior year recommendations. Implementing more of these recommendations will help CNCS to mature its information security program.

[10] Of the 58 open recommendations, 17 open recommendations from FY 2014 – FY 2018 are superseded by FY 2019 recommendations that remain open. We will close the 17 recommendations from the FY 2014 – FY 2018 with the issuance of this report.
[11] The CNCS's financial system.

To address the continuing weaknesses in CNCS's information security program and practices, we have provided eight new recommendations and one modified repeat recommendation that will assist CNCS in addressing challenges in its development of a mature and effective information security program.

FISMA Evaluation Findings

The existing weaknesses identified in this evaluation align with the particular security domains, as summarized in **Table 3,** which details the weaknesses mapped to the IG FISMA Metric Domains. The existing weaknesses include both the findings noted in the FY 2020 FISMA evaluation and the prior years' (PY) recommendations that remain open, detailed in **Appendix III**.

Table 3: Cybersecurity Framework Security Functions mapped to existing weaknesses noted in the FY 2020 FISMA Evaluation of CNCS

FY 2020 IG FISMA Metric Domain	Existing Weaknesses
Risk Management	Unpatched and unsupported software **(Finding 1)**
	Insufficient information technology asset inventory management **(Finding 2)**
	Lack of a mission and business risk registry (Open PY Recommendation)
	Insufficient mobile device management **(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)**
	Insufficient personnel screening process (Open PY Recommendation)
	Inadequate monitoring of wireless access connections (Open PY Recommendation)
	Inadequate physical controls (Open PY Recommendation)
Data Protection and Privacy	Lack of annual role-based privacy training (**Finding 7**)
	Insufficient protection of personally identifiable information (Open PY Recommendation)
Information Security Continuous Monitoring	Inadequate review and analysis of audit logs (Open PY Recommendation)

Management's Response and Evaluator's Comments

In response to the draft report, CNCS concurred with seven of the nine new and modified recommendations, but its proposed corrective actions did not respond fully to four of them. CNCS concurred with:

- Recommendation 1 to perform and document an oversight process to ensure physical inventory reviews and updates are fully documented. CNCS stated that the agency's future IT service contract will include a specific service level

agreement (SLA) that directly addresses the service provider's responsibility to maintain an accurate IT inventory. However, management's response did not include a process for its responsibility to monitor the contractor's performance on the SLA.

- Recommendation 3 to develop and implement a process to block unauthorized applications from installation on AmeriCorps mobile devices by August 2021.

- Recommendation 4 to complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations. Management stated they have finished configuring Nessus software to scan for baseline configurations.

- Recommendation 5 to fully implement standard baseline configurations for all platforms in the CNCS information technology environment and establish processes to test and monitor for compliance with established CNCS security standards. Management stated during fieldwork that it expects to complete this corrective action by the end of FY 2020, but they did not include that target date in the formal response.

- Recommendation 6 to assess and document a plan for reinstating mandatory enforcement of multifactor authentication as recommended by the Cybersecurity and Infrastructure Security Agency to address increased risks with a large number of personnel teleworking during the pandemic. Although CNCS states that it intends to enforce this requirement in the future, management did not provide either a corrective action plan or a targeted completion date.

- Recommendation 7 to ensure CNCS system administrators validate user accounts were approved before granting Momentum access. CNCS did not provide a targeted completion date.

- Recommendation 8 to ensure accounts for users that never logged in are included in the AmeriCorps Inactive script. CNCS did not provide a targeted completion date.

With respect to the remaining recommendations, CNCS:

- Concurred in part with Recommendation 2 pertaining to mobile device management. CNCS asserts that it currently requires mobile device users to install security and operating system updates on CNCS mobile devices within a prescribed time period. Management stated that they have the capability to deny access when a device is not updated. During fieldwork, management stated it would implement a new mobile device management tool during the first quarter of FY 2021 with the ability to automate updates and deny access. In their response to this report, management stated that the new tool will be implemented late in FY 2021.

CNCS provided no evidence that it requires installation of mobile device updates within a prescribed period, nor that it enforces any such deadlines by denying access to CNCS enterprise services for mobile devices on which updates have not been installed. Since CNCS has not yet automated this capability, they should in the meantime establish a deadline, monitor compliance and enforce it.

- Disagreed with Recommendation 9 pertaining to the completion of annual privacy role-based training. CNCS stated that personnel who handle significant Personally Identifiable Information (PII) received role-based privacy training in May 2019 and asserted that annual role-based privacy training is not required.

  NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations, control AR-5, Privacy Awareness and Training*, requires organizations to administer targeted, role-based privacy training to personnel responsible for PII and to those whose activities involve PII at least annually. Moreover, CNCS's internal documentation—the *CNCS Cybersecurity Control Families* document—requires that role-based privacy training be administered annually.

Lastly, management stated that our assessment of the Security Functions Respond and Recover did not find any weaknesses for these controls, which were rated at Level 3, Consistently Implemented. CNCS had identified areas of improvement for these functions to achieve the next maturity level, *Managed and Measurable*, in order to obtain an effective maturity program; but has not implemented the improvements.

CNCS's comments are included in their entirety in Appendix IV. We recommend that CNCS update and revise its corrective action plans for prior year recommendations and those newly issued, including target completion dates, so that its progress can be tracked and reported in the FY 2021 FISMA evaluation.

The following section provides a detailed discussion of the findings grouped by the Cybersecurity Framework Security Functions. Appendix I provides background information on CNCS and the FISMA legislation, Appendix II describes the evaluation scope and methodology, Appendix III summarizes the status of prior years' recommendations, and Appendix IV contains management comments.

Security Function: Identify

1. CNCS Must Improve its Vulnerability and Patch Management Controls

FY 2020 IG FISMA Metric Area: *Risk Management*

Patch management is the process of identifying, acquiring, installing, and verifying patches for products and systems, and is an important component of vulnerability management. Although our independent vulnerability scans indicated that the number of vulnerabilities averaged by host scanned has decreased by 37% since last year (**Figure 1**), the CNCS network continues to be exposed to critical and high severity vulnerabilities through unpatched software, improper configuration settings, and unsupported software. CNCS did not resolve critical vulnerabilities within seven days of occurrence and high-risk vulnerabilities within 30 days, as required by its internal operating policies. CNCS has still not resolved the configuration weaknesses from credential and non-credential scans that were published[12] before 2019.

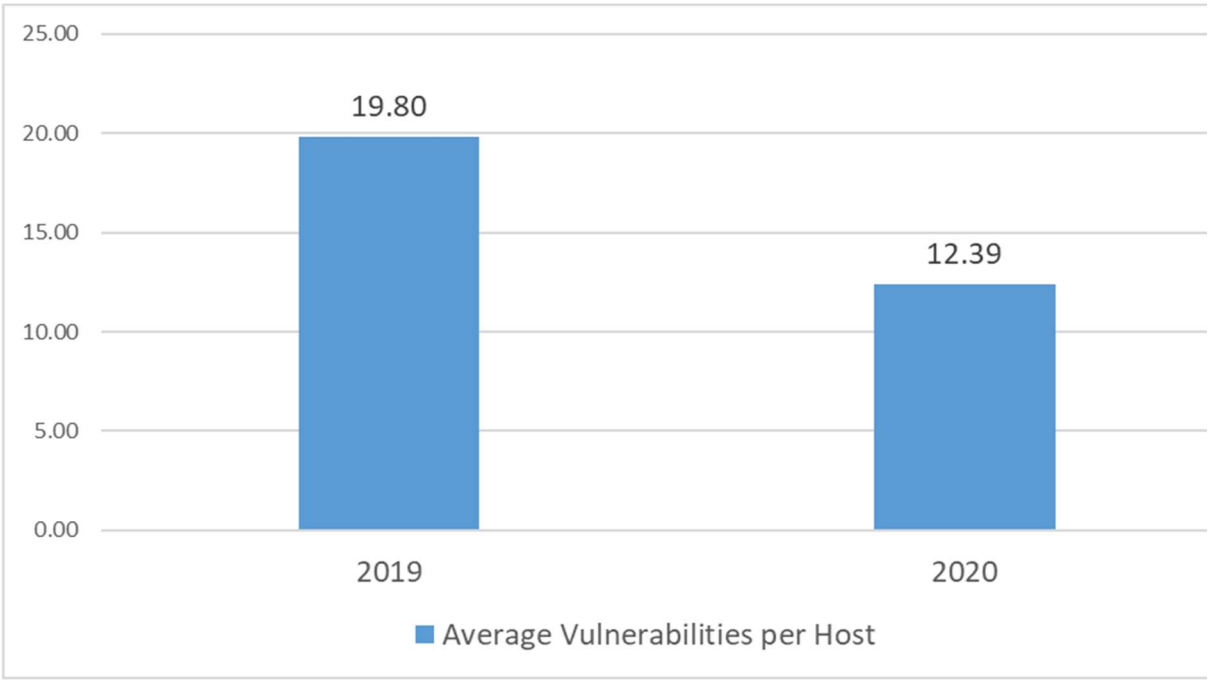

Figure 1. Comparison of the total number of critical and high-risk vulnerabilities identified by the independent auditors' credentialed vulnerability scans, averaged by host from FY 2019 and 2020.

[12] Configuration weaknesses are identified by Tenable Nessus Vulnerability Scanners by specific checks known as plugins and assigned a publication date. When assigned a publication date, these vulnerabilities are considered to be publicly known for use in vulnerability scanners.

Specifically, we noted patch management issues at the CNCS Headquarters (HQ), Washington, DC:

- From a non-credential scan of 876 systems at CNCS HQ, using the Tenable Nessus Vulnerability Scanner software tool, we identified **882 total critical and high-risk vulnerabilities** (190 critical and 692 high-risk) related to patch management, configuration management, and unsupported software. Of the total, 689 were caused by missing patches, 103 were caused by configuration weaknesses, and 90 were caused by unsupported software.
- Of the 110 systems scanned, 83 Windows servers and two workstations reported successful credential scans.[13] Of those 85 hosts on the CNCS HQ network, we identified **363 critical and 690 high-risk vulnerabilities** related to patch management, configuration management, and unsupported software. Of the 1,053 total critical and high-risk vulnerabilities, 929 were caused by missing patches, 23 were caused by configuration weaknesses, and 101 were caused by unsupported software. **Figures 3 and 4** depict CNCS HQ vulnerabilities by criticality and type.

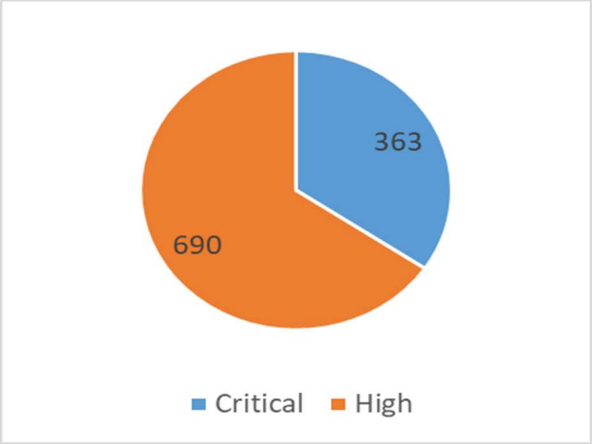

Figure 3 HQ total vulnerabilities by criticality from credentialed scans

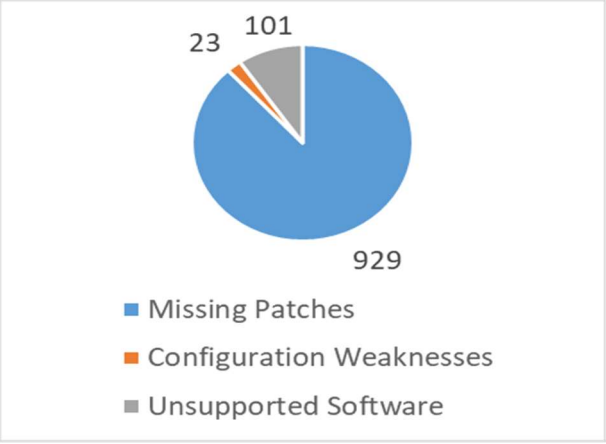

Figure 4 HQ total vulnerabilities by type from credentialed scans

- From the non-credential scans, 879 (99 percent) of the 882 critical and high-risk vulnerabilities were from 2019 or before. From the credential scans, 633 (60 percent) of the 1,053 critical and high-risk vulnerabilities were from 2019 or before.
- All of the configuration weaknesses from credential and non-credential scans were published before 2019 and were related to unprotected file shares and Windows services, Intelligent Platform Management Interface authentication disclosures, and Simple Network Management Protocol default community names.

[13] We attempted credential scans on 110 systems. The credentials provided by CNCS only succeeded on 85 systems. The other systems did not report a valid credential scan when reviewing CNCS scan results. The discrepancy is attributed to the configuration of the account provided to CLA rather than a reportable flaw of the CNCS vulnerability scanning process.

- The unsupported software was related to the following:
  - VMware ESX / ESXi unsupported version 6.0 as of March 12, 2020
  - VMware ESX version 4.1 unsupported as of May 21, 2014
  - Microsoft Exchange Server version 2007 SP3 unsupported as of April 11, 2017
  - Microsoft XML Parser and XML Core Services no longer supported as of April 12, 2014
  - Oracle WebLogic Server version 10.3.6.0 unsupported on January 1, 2017
  - Oracle Java JRE Version 1.6.0U45 unsupported on December 1, 2018

The overall deployment of vendor patches and system upgrades to mitigate the vulnerabilities was inconsistent and not effective for the CNCS HQ network. Specifically, CNCS did not effectively implement its process to ensure the timely correction of identified information system flaws, such as configuration weaknesses or unsupported software. Further, management stated the VMware servers are identified for decommissioning during the 1st quarter of FY 2021 and the latest version is being installed on new hardware. Management also stated that the Microsoft Exchange Server version 2007 is identified for decommissioning during the 3rd quarter of FY 2021 and is only accessible by a system account; no users access this server.

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;
- Employing vulnerability scanning tools and techniques that promote interoperability among tools and automate parts of the vulnerability management process by using standards for:
  1. Enumerating platforms, software flaws, and improper configurations;
  2. Formatting checklists and test procedures; and
  3. Measuring vulnerability impact;
- 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);
- Information system flaws are identified, reported, and corrected;
- Software and firmware updates related to flaw remediation are tested for effectiveness and potential side effects before installation;
- Security-relevant software and firmware updates are installed within the guidelines defined in security control RA-5 of the release of the updates; and

- Flaw remediation is incorporated into the organizational configuration management process.

The information systems at CNCS are at an elevated risk due to unpatched systems. A variety of critical vulnerabilities could be exploited using *unsophisticated* techniques to take control of systems, to cause a denial of service attack, or to allow unauthorized access to the CNCS systems and applications. In addition, operating system and application software that is missing security patches or software for which the vendor no longer maintains updated security patches leaves security weaknesses unfixed, exposing those systems to increased attack methods compromising the confidentiality, integrity, and availability of data.

The FY 2017,[14] 2018,[15] and 2019[16] FISMA evaluation reports included the following recommendations to assist CNCS in improving their vulnerability management program:

- Monitoring and promptly installing patches when they become available from the vendor;
- Replacing information system components when support is no longer available, and remediating or minimizing the impact of vulnerabilities on network devices;
- Monitoring and recording actions taken by the contractor to ensure vulnerability remediation for network devices and servers is addressed or the exposure minimized; and
- Enhancing the inventory process to ensure all devices are properly identified and monitored.

Although CNCS improved current patching since last year, there were still issues with applying older patches and remediating older configuration weaknesses. There were missing patches as far back as 2013 and older configuration weaknesses as far back as 2005. Based on the results of our independent scans, we noted management did not take corrective action on these recommendations. However, we closed the FY 2017 and 2018 recommendations because they are superseded by the FY 2019 recommendation. The FY 2019 recommendation remains open and we are not making additional recommendations at this time.

[14] Recommendation 24, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 31, (OIG Report No. 18-03, December 18, 2017).
[15] Recommendation 1, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 19-03, March 1, 2019).
[16] Recommendations 1, 2 and 3, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 10, (OIG Report No. 20-03, January 24, 2020).

Furthermore, prior-years' recommendations included evaluating the internet connections at the Field Financial Management Center (FFMC), National Civilian Community Corps (NCCC) Campuses, and State Offices[17] to determine if they are sufficient to allow patches to be deployed to all devices within the defined risk-based timelines. Management stated that the remediation of this recommendation is still ongoing, with a target completion date of September 2023; therefore, we are not making a new recommendation.

Finally, we closed as implemented a recommendation that CNCS Office of Information Technology (OIT) Infrastructure staff monitor the vulnerability scanning tool and validate vulnerability management activities on the networks and devices they manage.

2. CNCS Must Improve Its Inventory Management Process

FY 2020 IG FISMA Metric Area: *Risk Management*

NIST SP 800-53, Revision 4 requires the organization to develop and document an inventory of information system components that: 1) Accurately reflects the current information system, and 2) Includes all components within the authorization boundary of the information system. The CNCS *Cybersecurity Control Families* document requires the information system component inventory to be reviewed and updated at least annually.

CNCS did not maintain proper inventory management controls. Specifically, the inventory listing used to track the reassignment or relocation of IT assets was incomplete, as the new location was not documented for all assets. Applying adequate security controls to CNCS IT assets requires knowing what those assets are and where they are located.

The inventory management process is predominantly manual and involves HQ personnel updating the Configuration Management Database (CMDB) inventory and the FasseTrack system[18] when changes occur. CNCS management stated that an annual physical inventory of all hardware assets is usually conducted in April; however, due to COVID-19, the annual inventory was not scheduled and conducted this year. As a compensating control to a full physical inventory, an inventory listing was developed beginning in May 2020 to track IT assets that were reassigned or relocated. Management indicated the lack of detail related to all of the assets was due to an oversight and the listings would be updated to include the missing information.

[17] CNCS closed its State Offices except for the offices in Puerto Rico and Pennsylvania. The Pennsylvania state office transitioned to the Regional Office in September 2020. State Office functions were among those transferred to eight Regional Offices, six of which are now housed in temporary offices and two in permanent offices.

[18] FasseTrack is an asset management system for electronic tracking and maintenance of inventory.

Incomplete or inaccurate inventories could result in a loss of confidentiality, theft, 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.

The FY 2019 FISMA evaluation report[19] included the following recommendations to assist CNCS in improving the inventory management process:

- Implementing a process to ensure manual updates to the CMDB inventory and FasseTrack system are made simultaneously when the inventory is updated;
- Ensuring RemedyForce tickets are completed at the time the inventory is updated; and
- Performing periodic reconciliations between CMDB and the FasseTrack system.

Management stated these recommendations were scheduled to be completed in June 2020, but were not completed. Additionally, the recommendations included performing analysis to determine the feasibility of completely automating the inventory management process. Management stated the recommendation is scheduled to be completed in June 2021. Therefore, these recommendations remain open. To further assist CNCS in strengthening information system component inventory management controls, we recommend that CNCS:

> ***Recommendation 1:*** Perform and document an oversight process to ensure physical inventory reviews and updates are fully documented to include the exact location of all information technology assets. *(New)*

3. CNCS Must Improve Its Mobile Device Management Program

FY 2020 IG FISMA Metric Area: *Risk Management*

A mobile device is a hand-held computer such as a smartphone, tablet, or laptop. Mobile devices also require adequate protection to protect the confidentiality and integrity of CNCS data. CNCS did not effectively implement controls over mobile devices issued and authorized for official use, including for application management. Specifically, we noted:

- CNCS did not require mobile device users to install security and operating system updates within a prescribed period, or deny access to CNCS enterprise services by devices that were not updated within that prescribed period; and
- CNCS did not implement a process to prevent users from installing/downloading unauthorized software on their official mobile devices.

[19] Recommendations 4, 5, 7 and 7, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 10, (OIG Report No. 20-03, January 24, 2020).

CNCS management stated that its current mobile device management tool, which was adopted in July of 2015, does not have the capability to allow CNCS to implement these mobile device and application management controls. CNCS plans to implement these controls during the first quarter of FY 2021 via a new mobile device and application management tool. Furthermore, management stated that CNCS mobile devices are limited to synchronized email using the native email application on the mobile device, limiting access to any other CNCS information systems (e.g. Microsoft Office 365).

NIST SP 800-53, Revision 4, security control AC-19, states that the organization must establish usage restrictions, configuration requirements, connection requirements, and implementation guidance for organization-controlled mobile devices. In addition, Control Enhancement 4 of security control CM-7, recommends an allow-all, deny-by-exception policy to prohibit the execution of unauthorized software programs on the information system.

NIST SP 800-124, Revision 1, *Guidelines for Managing the Security of Mobile Devices in the Enterprise*, states the following:

> General security recommendations for any IT technology are provided in NIST SP 800-53. Policy restrictions of particular interest for mobile device security include the following:
>
> - Limit or prevent access to enterprise services based on the mobile device's operating system version.
> - Restrict which applications may be installed through whitelisting (preferable) or blacklisting.

Across government and the private sector, individuals rely increasingly on mobile devices for official communications and interface with office systems and networks. Without technical controls preventing the installation of potentially harmful software on CNCS mobile devices, employees may introduce potentially dangerous software and malware into the CNCS computing environment. In addition, without specifying how quickly users must apply available security and operating system updates, and without an automated tool to validate and enforce compliance, CNCS permits its mobile devices to remain vulnerable to potential security threats.

The FY 2017[20] FISMA evaluation report included recommendations to assist CNCS in improving the security of mobile devices at the Vicksburg and Denver NCCC campuses. Management stated that the recommendations are scheduled to be completed on September 30, 2020. These recommendations remain open. To further assist CNCS in strengthening mobile device management controls, we recommend that CNCS:

[20] Recommendations 25, 26, 27, and 29, *Fiscal Year 2017 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 31, (OIG Report No. 18-03, December 18, 2017).

Recommendation 2: Specify how quickly users must apply security and operating system updates on CNCS mobile devices, and implement a process to deny access to CNCS enterprise services for mobile devices that have not been updated within the prescribed period. *(New)*

Recommendation 3: Develop and implement a process to block unauthorized applications from installing on CNCS mobile devices. (New)

Security Function: Identify
Maturity Model Scoring

The 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)	6	2, 5, 6, 7, 10, and 12
Consistently Implemented (Level 3)	3	3, 9, and 11
Managed and Measurable (Level 4)	2	1 and 8
Optimized (Level 5)	1	4
Calculated Maturity Level: Defined (Level 2), Not Effective		

The FY 2020 IG FISMA 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[21] and 2019[22] FISMA evaluation reports 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.

CNCS performed a gap analysis and determined the corrective actions required to improve security controls for each IG FISMA Metric question to achieve the next maturity level for the Identity function area, *Consistently Implemented*. As CNCS reaches the *Consistently Implemented* maturity level, CNCS will need to continue to formulate action plans to achieve a maturity level of *Managed and Measurable* in order to achieve an effective information security program based on the IG FISMA Metrics. We closed the FY 2018 recommendation because it is superseded by the FY 2019 recommendation. The FY 2019 recommendation remains open and we are not making additional recommendations at this time.

[21] Recommendation 7, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 19-03, March 1, 2019).
[22] Recommendation 9, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 14 (OIG Report No. 20-03, January 24, 2020).

Security Function: Protect

4. CNCS Must Implement Standard Baseline Configurations

FY 2020 IG FISMA Metric Area: *Configuration Management*

Standard baseline configurations are security settings applied to information systems to decrease the risk of vulnerabilities being exploited. CNCS did not fully implement standard baseline configurations for all information system platforms. Specifically, we noted:

- Although the Corporation documented the standard baseline configurations for the information system components in their information technology environment, we were not able to validate that the standard baseline configurations were fully implemented, due to lack of evidence provided; and
- Our independent scans noted compliance of 65 to 85 percent with standard baseline configurations for Windows Server 2016 and Windows 10 workstations on the CNCS network, which also indicates that the configurations were not fully implemented.

CNCS management stated that OIT is in the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations in order to assess compliance. Management expects the baselines to be fully implemented by the end of the FY 2020.

The *CNCS Cybersecurity Control Families* document requires the ISSO to:

- Establish and document configuration settings for information technology products employed within the information system using the United States Government Configuration Baseline, NIST, National Security Agency, Center for Internet Security, or Defense Information Systems Agency security configuration checklists that reflect the most restrictive mode consistent with operational requirements;
- Implement the configuration settings;
- Identify and document exceptions from established configuration settings for individual components within the information system based on explicit operational requirements (note: exceptions must be approved by the Information Security Officer, Authorizing Official, and/or the Change Control Board); and
- Monitor and control changes to the configuration settings in accordance with organizational policies and procedures.

Information technology components that do not comply with standard baseline configurations increase the risk that a security vulnerability will be exploited. In addition, in the absence of appropriate monitoring, 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.

The FY 2017,[23] FY 2018,[24] and FY 2019[25] FISMA evaluation reports made recommendations for CNCS to 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, and track risk acceptances for deviations from standard configuration policy. We closed the FY 2017 and 2018 recommendations because they are superseded by the FY 2019 recommendation. The FY 2019 recommendation remains open.

During FY 2020, we validated that CNCS documented deviations from the standard configuration policies. However, CNCS is still in the process of validating compliance with the standard baseline configurations therefore, compliance reports were not available for us to validate implementation status. Management stated the expected completion date for fully implementing the baseline configurations is December 2020.

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

> ***Recommendation 4:*** *Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations. (New)*
>
> ***Recommendation 5:*** *Fully implement standard baseline configurations for all platforms in the CNCS information technology environment and establish processes to test, and monitor for compliance with established CNCS security standards. (Modified Repeat)*

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

FY 2020 IG FISMA Metric Area: *Identity and Access Management*

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 include tokens or PIV credentials issued by Federal agencies. In addition, NIST[26] requires information

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

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

[25] Recommendations 10, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 16, (OIG Report No. 20-03, January 24, 2020).

[26] *National Institute of Standards and Technology (NIST) Special Publication (SP) 800-53, Revision 4:* IA-2 Identification and Authentication (Organizational Users), Control Enhancement (1) Network Access to Privileged Accounts, Control Enhancement (2) Network Access to Non-Privileged Accounts, and Control Enhancement (3) Local Access to Privileged Accounts.

systems categorized as moderate-impact[27] 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. Lastly, OMB M-19-17, *Enabling Mission Delivery through Improved Identity, Credential, and Access Management*, issued May 21, 2019, states "Agencies shall require PIV credentials (where applicable in accordance with [Office of Personnel Management] OPM requirements) as the primary means of identification and authentication to Federal information systems and Federally controlled facilities and secured areas by Federal employees and contractors."

We noted the following issues regarding multifactor authentication:

- CNCS did not fully implement multifactor authentication (e.g., PIV cards) for local and network access for privileged users.[28] We discovered seven privileged users who were contractors without multifactor authentication.

  Management did not prioritize the implementation of multifactor authentication for privileged users as directed by OMB[29]. Management stated that CNCS started the process of issuing PIV cards to contractors using a prioritized list; contractors that had higher level privileges such as system administrators and help desk technicians were issued PIV cards first. Due to the large number of contractors that required processing, OIT and the Office of Human Capital (OHC) agreed to submit contractors for PIV badges in small groups. This approach allowed OHC to balance this with other office priorities and monitor the progress. Management stated that processing was almost completed for the contractors when COVID-19 closed all of the USAccess centers. As the USAccess centers are starting to reopen, OHC is processing Federal employees who started during COVID-19 to complete the process of issuing them PIV cards. Once that backlog is caught up, OHC will continue processing existing contractors.

  Failure to implement strong multifactor authentication for local and network access by privileged users significantly increases the risk of harm because those users have greater access to agency networks and systems. Unauthorized privileged access can allow an individual to inappropriately create, delete and modify users and services running on the network as well as gain access to all data stored on the network.

- Although multifactor authentication for network access was being implemented for non-privileged users on Microsoft Windows 10 workstations, certain non-privileged users are still using Windows 7 workstations for which multifactor authentication

[27] NIST defines a Moderate-Impact system as an information system in which at least one security objective (i.e., confidentiality, integrity, or availability) is assigned a FIPS 199 potential impact value of moderate, and no security objective is assigned a FIPS 199 potential impact value of high.

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

[29] The Federal Chief Information Officer initiated a 30-day Cybersecurity Sprint on June 12, 2015, led by OMB, instructing Federal agencies to dramatically accelerate implementation of multi-factor authentication, especially for privileged users.

was not and will not be implemented. For example, based on our review of the hardware asset inventory listing, we found 27 Windows 7 workstations assigned to CNCS users.

Management stated that the users whose workstations were not upgraded to Windows 10 were remote users, and the Windows 10 laptops are being deployed as regional offices are opening. Management also indicated that if a former Office of Field Liaison (OFL) employee is transitioning to a new regional office position, they are issued a Windows 10 laptop. If the OFL employee is not transitioning, they will continue to use their Windows 7 device until their employment with CNCS ends. Without strong multifactor authentication for network access for non-privileged user accounts, there is increased risk of unauthorized access to CNCS information and information systems by an unauthorized user decreasing the confidentiality and integrity of data.

- CNCS removed mandatory enforcement of PIV authentication in March 2020 as a way for facilitating remote access during to the COVID-19 pandemic. CNCS management reached this decision without conducting and documenting a risk assessment or formally accepting the associated risks, until CLA brought this issue to management's attention. In response to increased risks with the large number of Federal personnel teleworking due to the pandemic, the Cybersecurity and Infrastructure Security Agency alert AA20-073A, March 13, 2020, recommended among other things, requiring multifactor authentication for all users.

  Management stated that the removal of mandatory enforcement of PIV authentication was a technical change to allow uninterrupted telework access in the event a user had PIV-related issues during to the COVID-19 pandemic. Management was concerned that users would not be able to obtain a new PIV card should their card become damaged or lost since most personnel were working remotely. Management stated that in order to lessen the downtime for users, it would be faster for the help desk personnel to advise the user to log in with their network password rather than modifying the laptop settings to disable PIV requirements on a case-by-case basis. Management believed that most users would continue to use their PIV cards as staff were not advised of the change unless they reached out to the help desk because of a problem.

  On August 10, 2020 and again on September 30, 2020, CNCS extended its Phase I period for reopening its offices. Without multifactor authentication in place during these extended periods of telework, the risks of unauthorized access are increased. The more time hackers have to gain information about CNCS users and systems, the success rate of gaining unauthorized access increases. In addition, without multifactor authentication, there is an increased risk that security controls, such as firewalls and malicious code/program detection software, can be bypassed, allowing access to sensitive CNCS information. As a result, CNCS information systems are at increased risk for disruption of operation, leading to loss of productivity. In addition, the Corporation may be exposed to inappropriate

or unauthorized access to sensitive information, including PII which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach of PII. Subsequently, the Corporation's current information system environment will require strong cybersecurity measures to remediate the heightened risks and safeguard assets against potential security threats.

The FISMA evaluations for FY 2017,[30] FY 2018,[31] and 2019[32] each recommended that CNCS implement PIV multifactor authentication for local and network access for privileged users, and implement PIV multifactor authentication for network access for non-privileged users. Management stated that these recommendations were scheduled to be completed in June 2020; however, we determined that these recommendations were not fully implemented. We closed the FY 2017 and 2018 recommendations because they are superseded by the FY 2019 recommendations. The FY 2019 recommendations remain open and we are not making additional recommendations at this time. However, we are making a new recommendation regarding removing mandatory enforcement of PIV authentication during the COVID-19 pandemic. We recommend CNCS:

> ***Recommendation 6:*** Assess and document a plan for reinstating mandatory enforcement of multifactor authentication as recommended by the Cybersecurity and Infrastructure Security Agency to address increased risks with the large number of personnel teleworking during the pandemic. *(New)*

6. CNCS Must Strengthen Account Management Controls

FY 2020 IG FISMA Metric Area: *Identity and Access Management*

CNCS did not effectively manage user accounts and/or passwords. For example, CNCS officials did not approve all Momentum accounts, disable network accounts of separated employees and inactive accounts, 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.

[30] 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).

[31] 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. 198-03, March 1, 2018).

[32] Recommendations 11 and 12, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 18, (OIG Report No. 20-03, January 24, 2020).

Specifically, the following issues were noted:

Lack of Account Approvals:

- One new Momentum user account from a sample of five Momentum user accounts, created on March 9, 2020, did not have documentation of the approval to create the account, as required by the CNCS policy, *Cybersecurity Control Families*. Upon notification, management disabled the account on July 22, 2020 to process a new access request form in attempt to document the approval.

  Management did not have oversight to ensure all Momentum accounts were authorized prior to being created. Management indicated that Momentum will no longer be the CNCS financial system of record on October 1, 2020. All financial records will be managed and maintained within the U.S. Treasury Bureau of the Fiscal Service shared service environment. However, Momentum will not be fully decommissioned until the details are worked out on how the shared services will continue to provide information to the CNCS Electronic-Systems for Program Agreements and National Service Participants (eSPAN) system. Until such time, Momentum will still function as a CNCS FISMA information system, with limited access. Without documenting approvals to create new users' system accounts, the risk of inappropriate and/or unauthorized access to the Corporation's information system environment is increased. Furthermore, this heightens the risk of the unauthorized modification, loss, and disclosure of sensitive and/or critical CNCS information.

Weaknesses in Account Management for Separated Employees:

- One out of the total population of 46 Federal contractors who separated from CNCS service between October 1, 2019 and May 1, 2020, still maintained access to the My AmeriCorps Staff Portal Active Directory Organizational Unit (OU),[33] for nine days following the individual's date of separation. CNCS policy requires disabling system accounts within one working day following separation. We noted that the network account was disabled for this individual.

  Management had not established appropriate oversight to ensure that the application account for the terminated personnel was removed from the My AmeriCorps Staff Portal Active Directory OU at the same time the network account was disabled. If a separated individual's disabled network accounts are not removed from the My AmeriCorps Staff Portal OU, and the active directory accounts are purposefully or inadvertently re-enabled, access to My AmeriCorps Staff Portal is maintained. There is a risk that these accounts could be accessed by unauthorized users.

[33] My AmeriCorps Portal is a web-based application under CNCS's network used to communicate AmeriCorps member enrollment and service completion data to the National Service Trust. An OU is a subdivision in Active Directory to hold users, groups, and computers with designated Group Policy settings and account permissions.

The FISMA evaluation for FY 2019[34] recommended that CNCS monitor the employee separation process to ensure CNCS policy is followed for disabling system accounts for separated employees, including removing accounts of separated individuals from the My AmeriCorps Staff Portal OU. Based on the results of our testing, indicating a separated contractor maintained access to the My AmeriCorps Staff Portal OU, we concluded this prior year recommendation remains open.

Improper Management of Inactive Accounts:

- Two network accounts (one non-privileged account included in the Pilot OU and one privileged account included in the OIT OU), did not log in within 30 days, but the accounts were not disabled in accordance with CNCS policy, *Cybersecurity Control Families*. This occurred because the inactive account script was not configured to include all OUs. Therefore, accounts in the Pilot and OIT OUs were not disabled due to inactivity.

- Four non-privileged network accounts that did not log in within 30 days were not disabled in accordance with CNCS policy, *Cybersecurity Control Families*. The four non-privileged network accounts that did not log in within 30 days were accounts that were created for employees who never onboarded. The inactive account script did not identify and disable the accounts for the users who never logged in.

  Although inactive user accounts are dormant, they still retain access to systems and data posing a target for exploitation. Unauthorized users can use a dormant account to gain access to the Corporation's information systems.

Weaknesses in Password Management:

- One non-privileged network account included in the Pilot OU did not have a password change within 90 days but was not disabled in accordance with CNCS policy, *Cybersecurity Control Families*. The CNCS password script was not configured to include all OUs. Therefore, accounts in the Pilot OU were not disabled due to passwords that exceeded the allowed timeframe. Without changing passwords consistently, the risk is increased that an unauthorized user targeting these accounts will have frequent access to the accounts. Regular password changes limit the period of exposure should the account be compromised.

  The FISMA evaluation for FY 2019[35] recommended that CNCS monitor automated scripts to validate that accounts are disabled after 30 days of inactivity in accordance with CNCS policy, and to ensure all CNCS information system passwords are changed at the frequency specified in applicable CNCS policy or the System Security Plan. Since our testing indicated continuing issues with the

[34] Recommendation 13, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 20, (OIG Report No. 20-03, January 24, 2020).

[35] Recommendations 14 and 16, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 20, (OIG Report No. 20-03, January 24, 2020).

inactive accounts and password scripts, the prior recommendation remains open, and we are making a new recommendation to address accounts that never logged in.

NIST SP 800-53, Revision 4 requires CNCS to create, enable, modify, disable, and remove information system accounts in accordance with CNCS' defined procedures. Furthermore, CNCS is required to 1) automatically disable the account when the accounts have expired, 2) are no longer associated to a user, 3) are in violation of organizational policy, and 4) are no longer used by applications, services, or the system, and 5) have been inactive for a time-period defined by CNCS. In addition, CNCS is to manage information system authenticators by changing or refreshing authenticators within the organization's defined time-period.

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

- The System Administrator is responsible for creating, enabling, modifying, disabling, and removing information system accounts in accordance with CNCS Policy and system procedures.
- The Information Security Officer (ISO), upon termination of individual employment, is responsible for ensuring information system access is disabled within one 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 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 improper modification, loss, and unauthorized disclosure.

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

Recommendation 7: Ensure CNCS system administrators validate user accounts are approved prior to granting Momentum access. *(New)*

Recommendation 8: Ensure that accounts for users that never logged in are included in the CNCS Inactive script. (New)

7. CNCS Must Ensure Role-based Privacy Training Is Conducted Annually

FY 2020 IG FISMA Metric Area: *Data Protection and Privacy*

NIST SP 800-53, Revision 4, control AR-5, Privacy Awareness and Training, requires organizations to administer targeted, role-based privacy training for personnel having responsibility for PII or for activities that involve PII at an organization-defined frequency, **at least annually**. The *CNCS Cybersecurity Control Families* document requires role-based privacy training be administered annually for personnel having responsibility for PII or for activities that involve PII.

CNCS did not conduct role-based privacy training annually as required by CNCS policy. Role-based privacy training was administered in May 2019; CNCS did not schedule or conduct the training in FY 2020.

Management stated that during the current year, CNCS was managing major organizational changes, such as the opening up the new regional offices and transitioning its financial system to Federal Shared Services. The employees who would have received the targeted privacy training were major players in these organizational transitions. Management stated that by delaying training until the new fiscal year allowed those individuals to focus on completing more urgent tasks.

Furthermore, role-based privacy training was conducted for the first time in May 2019. Management stated there is a limitation within the learning management system that prevents individuals from taking mandatory training twice in a twelve-month period. Since the targeted training was completed in May 2019, those same individuals could not be assigned the training in October 2019 during the annual training cycle that occurs from October to November of each year. Management stated that a decision was made to delay targeted privacy training until October 2020 due to these reasons.

Without providing annual role-based privacy training to individuals with PII and privacy program management responsibilities, those personnel did not receive the appropriate more detailed training about processes for managing privacy, proper handling, and reporting. CNCS may be at increased risk of mishandling PII, potentially causing a breach resulting in increased costs in resources and damage to the Corporation's reputation. Particularly with the high number of employees new to CNCS, the failure to conduct role-based training posed a widespread risk.

To assist CNCS in strengthening the privacy program, we recommend CNCS:

> ***Recommendation 9:*** Ensure all personnel whose responsibilities include access to PII complete annual privacy-role based training. *(New)*

Security Function: Protect
Maturity Model Scoring

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

Function	Count	IG FISMA Metric Questions
Ad Hoc (Level 1)	1	20
Defined (Level 2)	13	15, 16, 17, 18, 19, 23, 24, 25, 26, 28, 29, 30, and 37
Consistently Implemented (Level 3)	4	21, 33, 35, and 36
Managed and Measurable (Level 4)	8	14*, 31, 34, 39*, 41, 42, 43 and 44
Optimized (Level 5)	2	27 and 40
Calculated Maturity Level: Defined (Level 2), Not Effective		

* The maturity scale for Questions 14 and 39 stopped at "Managed and Measurable." Therefore CNCS's "Managed and Measureable" maturity level on those questions was the highest available rating.

The FY 2018[36] and 2019[37] FISMA evaluation reports 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.

CNCS performed a gap analysis and determined the corrective actions required to improve security controls for each IG FISMA Metric question to achieve the next maturity level for the "Protect" function area, *Consistently Implemented*. As CNCS reaches the *Consistently Implemented* maturity level, it will need to develop action plans to achieve a maturity level of *Managed and Measurable* in order to achieve an effective information security program based on the IG FISMA Metrics. We closed the FY 2018 recommendation because it is superseded by the FY 2019 recommendation. The FY 2019 recommendation remains open and we are not making additional recommendations at this time.

[36] Recommendation 21, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 19-03, March 1, 2019).

[37] Recommendation 29, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 14 (OIG Report No. 20-03, January 24, 2020).

Security Function: Detect
Maturity Model Scoring

The 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[38] and 2019[39] FISMA evaluation reports included 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.

CNCS performed a gap analysis and determined the corrective actions required to improve security controls for each IG FISMA Metric question to achieve the next maturity level for the "Detect" function area, *Defined*. As CNCS reaches the *Defined* maturity level, CNCS will need to continue to formulate action plans to achieve a maturity level of *Managed and Measurable* in order to obtain an effective information security program based on the IG FISMA Metrics. We closed the FY 2018 recommendation because it is superseded by the FY 2019 recommendation. The FY 2019 recommendation remains open and we are not making an additional recommendation at this time.

Security Function: Respond
Maturity Model Scoring

Our judgmental assessment did not find any weaknesses for controls evaluated in the "Respond" function. The 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

[38] Recommendation 23, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 19-03, March 1, 2019).

[39] Recommendation 31, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 14 (OIG Report No. 20-03, January 24, 2020).

Function	Count	IG FISMA Metric Questions
Managed and Measurable (Level 4)	2	53* and 57*
Optimized (Level 5)	0	N/A
Calculated Maturity Level: Consistently Implemented (Level 3), Not Effective		

* The maturity scale for Questions 53 and 57 stopped at "Managed and Measurable." Therefore CNCS's "Managed and Measureable" maturity level on those questions was the highest available rating.

The FY 2018[40] and 2019[41] FISMA evaluation reports 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.

CNCS performed a gap analysis and determined the corrective actions required to improve security controls for each IG FISMA Metric question in the "Respond" function to achieve the next maturity level, *Managed and Measurable*, to obtain an effective maturity program. We noted the prior year recommendation is closed.

Security Function: Recover
Maturity Model Scoring

Our judgmental assessment did not find any weaknesses for controls evaluated in the "Recover" function. The 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		

* The maturity scale for Questions 62 and 65 stopped at "Consistently Implemented." Therefore CNCS's "Consistently Implemented" maturity score on those questions was the highest available rating.
** The same is true of Question 60, where CNCS's "Managed and Measurable" maturity score was the highest available rating.

[40] Recommendation 24, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 19-03, March 1, 2019).
[41] Recommendation 32, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 14 (OIG Report No. 20-03, January 24, 2020).

The FY 2018[42] and 2019[43] FISMA evaluation reports included 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.

CNCS performed a gap analysis and determined the corrective actions required to improve security controls for each IG FISMA Metric question in the "Recover" function to achieve the next maturity level, *Managed and Measurable*, to obtain an effective maturity program. We noted the prior year recommendation is closed.

[42] Recommendation 25, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, (OIG Report No. 19-03, March 1, 2019).

[43] Recommendation 33, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, page 14 (OIG Report No. 20-03, January 24, 2020).

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, AmeriCorps Health Benefits, AmeriCorps Childcare Benefits System, and public websites. The first five of these systems are categorized as moderate security, while the public websites are rated as low security.[44] 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 FFMC, and four NCCC campuses. These facilities are connected through commercially managed telecommunications network connections.

In 2019, CNCS closed its state offices except for the Puerto Rico and Pennsylvania offices. It has created eight Regional Offices, six of which are housed in temporary space and two in permanent offices. The Pennsylvania state office transitioned to a Regional Office in September 2020. Each Regional Office provides administrative management of grants within their region.

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 information systems.

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 Chief Information Security Officer, 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 *CNCS Cybersecurity Control Families* document, which incorporates the NIST SP 800-53, Revision 4.

[44] 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.

Appendix I

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.

Federal agencies are to provide information security protections commensurable 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 IG 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 2020 IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 19, 2019, OMB issued Memorandum M-20-04, *Fiscal Year 2019-2020 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 2020 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.[45]

The FY 2020 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,

[45] https://www.cisa.gov/publication/fy20-fisma-documents

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 2020 IG FISMA Metric Domains

NIST Cybersecurity Framework Security Functions	FY 2020 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

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

Appendix II

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.[46] 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

The evaluation was conducted remotely due to the restrictions caused by the COVID-19 pandemic from April 15, 2020 to October 16, 2020. A network vulnerability assessment was also conducted at HQ.

In addition, the evaluation included an assessment of effectiveness for each of the eight FY 2020 IG FISMA Metrics Domains and the maturity level of the five Cybersecurity Framework Security Functions. The evaluation also included a follow up on prior years' recommendations to determine whether CNCS made progress in implementing the recommended improvements concerning its information security program.[47]

[46] https://www.ignet.gov/sites/default/files/files/committees/inspect-eval/iestds12r.pdf
[47] *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, (OIG Report No. 20-03, January 24, 2020).

Appendix II

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 2020 IG FISMA Metrics Domains aligned with the Cybersecurity Framework Security Functions.[48] **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[49]
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.
- Tested system processes to determine the adequacy and effectiveness of selected controls.

[48] Security controls are organized into families according to their security function—for example, access controls.
[49] These associated controls are from NIST 880-53, Revision 4, located at https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf

- Reviewed the status of recommendations in the FY 2019 FISMA report, including supporting documentation, to ascertain whether the actions taken addressed the weakness.[50]

In addition, our work in support of the evaluation was guided by applicable CNCS policies and federal criteria, including, but not limited to, the following:

- Memorandum M-20-04, *Fiscal Year 2019-2020 Guidance on Federal Information Security and Privacy Management Requirements*.
- FY 2020 IG FISMA Reporting Metrics.
- NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations,* for specification of security controls.
- NIST SP 800-37, Revision 2, *Guide for Applying the Risk Management Framework to Federal Information Systems,* for the risk management framework controls.
- NIST SP 800-53A, Revision 4, *Assessing Security and Privacy Controls in Federal Information Systems and Organizations,* for the assessment of security control effectiveness.
- NIST Framework for Improving Critical Infrastructure Cybersecurity (Cybersecurity Framework).

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.

[50] Ibid 47.

Appendix III

STATUS OF PRIOR YEARS' RECOMMENDATIONS

The following tables summarize our follow up related to the status of open prior years' recommendations reported in the FY 2014, 2016, 2017, 2018, and 2019 FISMA evaluations.[51] [52] [53] [54] [55] There were no open recommendations from the FY 2015 FISMA evaluation.

During FY 2020, CNCS implemented corrective actions to close 11 prior years' recommendations from the FY 2014, 2016, 2017, 2018, and 2019 FISMA evaluations. An additional 17 open recommendations from FY 2014 – FY 2018 were closed because they were superseded by FY 2019 recommendations that remain open.

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:		
	Part B: Addressing and capturing risk at the mission/business process level (i.e., Tier 2), including clearly assigning ownership and responsibilities for executing risk management processes at this level.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 8.
	Part C: Integrating Tier 1 and 2 Level activities and linking them to Tier 3 Level activities related to implementation, operation, and monitoring of Corporation information systems.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 8.

[51] *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).
[52] *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).
[53] 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).
[54] 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).
[55] Ibid 47.

Appendix III

Status of Prior Year FY 2016 Recommendations

FISMA NFRs	FY 2016 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY16 – FISMA – NFR 1	**Recommendation 3:** Implement a process to maintain configuration baselines for desktops, servers and other network equipment that records installed software, software versions, and configuration settings as required by NIST SP 800-53, CM-2 Baseline Configuration.	Open	Closed This recommendation is superseded by FY 2019 recommendation 10.
	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.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 10.
	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.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 10.

Appendix III

Status of Prior Year FY 2017 Recommendations

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY17-FISMA-NFR 8	**Recommendation 7:** Complete the development, documentation, and communication of an organization-wide risk management strategy associated with the operation and use of the Corporation's information systems in accordance with NIST standards. This should include: • Finalizing the risk register • Establishing the risk tolerance for the Corporation, including information security and privacy, and communicating the risk tolerance throughout the organization • Developing, documenting, and implementing acceptable risk assessment methodologies, risk mitigation strategies, and a process for consistently evaluating risk across the organization with respect to the organization's risk tolerance • Developing, documenting, and implementing approaches for monitoring risk over time	Closed	Closed This recommendation is superseded by FY 2019 recommendation 8.
FY17-FISMA-NFR 5	**Recommendation 8:** Ensure that standard baseline configurations for all platforms in the CNCS information technology environment are appropriately implemented, tested, and monitored for compliance with established CNCS security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Open	Closed This recommendation is superseded by FY 2019 recommendation 10.
FY17-FISMA-NFR 9	**Recommendation 14**: Implement PIV multifactor authentication for local and network access for privileged users.	Open	Closed This recommendation is superseded by FY 2019 recommendation 11.

Appendix III

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY17-FISMA-NFR 9	**Recommendation 15**: Implement PIV multifactor authentication for network access for non-privileged users.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 12.
FY17-FISMA-NFR 1	**Recommendation 24:** Ensure the CNCS Office of Information Technology monitor and promptly install patches and antivirus updates when they are available from the vendor across the enterprise. Enhancements should include: • Improve the effectiveness of patching network devices and servers. • Ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer. • Ensure vulnerability remediation for network devices and servers is addressed or the exposure to unpatchable vulnerabilities is minimized. • Monitor and enforce Team Lead laptops' compliance with security updates and update of antivirus signatures.	Open	Closed This recommendation is superseded by FY 2019 recommendation 1.
	Recommendation 25: Ensure the CNCS GSS Information System Owner establishes and enforces the policy for mobile devices that do not connect to the CNCS GSS to include usage restrictions, configuration and connection requirements, and implementation guidance.	Open	Remains Open, Refer to Finding 3 We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.

Appendix III

FISMA NFRs	FY 2017 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	Recommendation 26: Ensure the facilities implement the following in regard to protection of mobile devices: • Enforce the prohibition of displaying passwords in public view • Require the use of passwords on mobile computer assets for all users • Change passwords and re-image IT assets upon the separation of the previous user • Monitor Team Lead laptops for compliance with security updates and antivirus signatures • Prohibit the use of non-governmental CNCS issued email accounts • Configure cell phones to require the enabling of security functions	Open	Remains Open, Refer to Finding 3 We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	Recommendation 27: Ensure the facilities implement the following in regards to protection of mobile devices: • Require the use of passwords on mobile computer assets for all users • Change passwords and re-image IT assets upon the separation of the previous user • Prohibit the use of non-governmental CNCS issued email accounts	Open	Remains Open, Refer to Finding 3 We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	Recommendation 29: Configure CNCS issued laptops to deny the use of the FEMA wireless network by service set identifier (SSID).	Closed	Closed

Appendix III

Status of Prior Year FY 2018 Recommendations

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY18 – FISMA – NFR 6	**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:		
	Part A: Implement a process to track patching of network devices and servers by the defined risk-based patch timelines in CNCS policy.	Open	Closed This recommendation is superseded by FY 2019 recommendation 1.
	Part B: Ensure replacement of information system components when support for the components is no longer available from the developer, vendor or manufacturer.	Open	Closed This recommendation is superseded by FY 2019 recommendation 1.
	Part C: 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.	Open	Closed This recommendation is superseded by FY 2019 recommendation 1.
	Part D: Enhance the inventory process to ensure all devices are properly identified and monitored.	Open	Closed This recommendation is superseded by FY 2019 recommendation 1.
	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	Open	Remains Open Refer to Finding 1

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	be inadequate, develop and implement a plan to enhance the current internet connections.		
FY18-FISMA-NFR 9	**Recommendation 4:** Develop and document a comprehensive risk register at the mission and business process level.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 8.
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.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 9.
FY18-FISMA-NFR 10	**Recommendation 8:** Ensure that standard baseline configurations for all platforms in the CNCS information technology environment are appropriately implemented, tested, and monitored for compliance with established CNCS security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Open	Closed This recommendation is superseded by FY 2019 recommendation 10.
FY18-FISMA-NFR 4	**Recommendation 11**: Implement Personal Identification Verification multifactor authentication for local and network access for privileged users.	Open	Closed This recommendation is superseded by FY 2019 recommendation 11.
	Recommendation 12: Implement Personal Identification Verification	Open	Closed

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	multifactor authentication for network access for non-privileged users.		This recommendation is superseded by FY 2019 recommendation 12.
	Recommendation 20: Require FFMC and the Vinton NCCC campus to conduct and document a physical security risk assessment.	Closed	Closed
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.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 29.
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.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 31.
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	Closed	Closed

Appendix III

FISMA NFRs	FY 2018 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	which addresses the corrective actions necessary to show steady, measurable improvement towards becoming an effective information security program.		
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.	Closed	Closed

Appendix III

Status of Prior Year FY 2019 Recommendations

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY19-FISMA-NFR 11	**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. • Ensure 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. • Enhance the inventory process to ensure all devices are properly identified and monitored.	Open	Remains Open Refer to Finding 1
	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.	Open	Remains Open Refer to Finding 1

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	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.	Closed	Closed
FY19-FISMA-NFR 6	**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.	Open	Remains Open Refer to Finding 2
	Recommendation 5: Develop and implement a written process to ensure RemedyForce tickets are completed at the time the inventory is updated.	Open	Remains Open Refer to Finding 2
	Recommendation 6: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.	Open	Remains Open Refer to Finding 2
	Recommendation 7: Perform and document analysis to determine the feasibility of completely automating the inventory management process.	Open	Remains Open Refer to Finding 2
FY19-FISMA-NFR 7	**Recommendation 8:** Continue the current effort to complete a comprehensive risk register at the mission and business process level.	Closed	Remains Open CNCS did not complete the mission/business process level risk register.

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY 19 FISMA Report	**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.	Closed	Remains Open Refer to Security Function: Identify Maturity Model Scoring
FY19-FISMA-NFR 9	**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.	Open	Remains Open Modified Repeat, refer to Finding 4
FY19-FISMA-NFR 8	**Recommendation 11:** Implement Personal Identification Verification multifactor authentication for local and network access for privileged users to all workstations and servers.	Open	Remains Open Refer to Finding 5
	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.	Open	Remains Open Refer to Finding 5

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY19-FISMA-NFR 1	**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.	Open	Remains Open Modified Repeat, refer to Finding 6
	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.	Open	Remains Open Modified Repeat, refer to Finding 6
	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.	Closed	Closed
	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.	Open	Remains Open Modified Repeat, refer to Finding 6
FY19-FISMA-NFR 2	**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.	Closed	Closed
FY19-FISMA-NFR 5	**Recommendation 18:** Complete background investigations in accordance with the developed schedule based on prioritization of higher-level risk.	Open	Remains Open Management stated that corrective action was not completed.

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	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.	Open	Remains Open Management stated that corrective action was not completed.
	Recommendation 20: Develop and implement a written process to ensure the Office of Human Capital completes background investigations for all contractors.	Open	Remains Open Management stated that corrective action was not completed.
FY19-FISMA-NFR 4	**Recommendation 21:** Assess the NCCC campus member credentialing process and mechanism to ensure compliance with CNCS personnel security policy for badging.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	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.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	Recommendation 23: Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	Recommendation 24: Periodically provide training for the NCCC campus personnel on the data retention and disposal requirements.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
	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.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
FY19-FISMA-NFR 3	**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.	Closed	Closed
	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.	Closed	Closed

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
	Recommendation 28: Secure the networking infrastructure located at the NCCC Southwest Region Campus in a locked room or cage.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.
FY 19 FISMA Report	**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.	Closed	Remains Open Refer to Security Function: Protect Maturity Model Scoring
FY19-FISMA-NFR 10	**Recommendation 30:** Develop and implement a written process to review and analyze the wireless network logs at the NCCC Pacific and Southwest Regional Campuses.	Open	Remains Open We did not revisit the CNCS sites where the issues were found to validate corrective action was completed at those sites. Management stated that corrective action was not completed.

Appendix III

FISMA NFRs	FY 2019 FISMA Evaluation	Status Determined by CNCS	Auditor Position on Status of Recommendations
FY 19 FISMA Report	**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.	Closed	Remains Open Refer to Security Function: Detect Maturity Model Scoring
FY 19 FISMA Report	**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.	Closed	Closed
FY 19 FISMA Report	**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.	Closed	Closed

Appendix IV

MANAGEMENT COMMENTS

To: Monique Colter, Assistant Inspector General for Audit

From: Pape Cisse, Chief Information Officer (CIO) Pape Cisse Digitally signed by NDIOGOU CISSE DN: c=US, o=U.S. Government, ou=Corporation for National and Community Service, cn=NDIOGOU CISSE, 0.9.2342.19200300.100.1.1=#0c7710001864512 Date: 2020.11.24 13:46:20 -05'00'

Terrence King, Acting Chief Information Security Officer (CISO) TERRENCE KING Digitally signed by TERRENCE KING Date: 2020.11.24 13:41:56 -05'0

Cc: Lisa Guccione, Chief of Staff
Scott Hefter, Chief Operating Officer
Helen Serassio, Acting General Counsel

Date: November 24, 2020

Subject: Response to Office of Inspector General's Draft Report: Fiscal Year 2020 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 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service[1].

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

Security Function: Identify
The maturity level based on the 12 IG FISMA Metrics questions for the "Identify" function is Level 2 (*Defined*), Not Effective.

1. CNCS Must Improve its Vulnerability and Patch Management Controls

Management stated that the remediation of this recommendation is still ongoing, with a target completion date of September 2023; therefore we are not making a new recommendation.

[1] Since the issuance of the draft report, the Corporation for National and Community Service has adopted the operating name of AmeriCorps.

AmeriCorps Response: AmeriCorps concurs. As the agency procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with Office of Information Technology (OIT)policies and procedures.

2. CNCS Must Improve Its Inventory Management Process

Recommendation 1: Perform and document an oversight process to ensure physical inventory reviews and updates are fully documented to include the exact location of all information technology assets. (New)

AmeriCorps Response: AmeriCorps concurs. As the agency procures a new IT service contract, there will be specific SLA in place that directly address the service provider's responsibility to maintain an accurate IT inventory.

3. CNCS Must Improve Its Mobile Device Management Program

Recommendation 2: Specify how quickly users must apply security and operating system updates on CNCS mobile devices and implement a process to deny access to CNCS enterprise services for mobile devices that have not been updated within the prescribed period. (New)

AmeriCorps Response: AmeriCorps concurs with specifying a time. AmeriCorps will develop policies to ensure system updates are implemented in a timely fashion. AmeriCorps is implementing Microsoft Intune to manage mobile devices. Intune is expected to be deployed by August 2021.

AmeriCorps non-concurs with implementing a process to deny access. AmeriCorps does have a process for denying access to its mobile devices. AmeriCorps does require mobile device users to install security and operating system updates within a prescribed period. AmeriCorps provided evidence that it has the capability to deactivate phones if updates are not installed and has provided evidence that this capability has been

used in the past. Mobile devices are critical to AmeriCorps users to conduct their day-to-day business, so AmeriCorps allows its users a substantial window of time to install updates.

Recommendation 3: Develop and implement a process to block unauthorized applications from installing on AmeriCorps mobile devices. (New)

AmeriCorps Response: AmeriCorps concurs. AmeriCorps is implementing Microsoft Intune to manage mobile devices. Intune is expected to be deployed in August 2021. Intune is covered under our existing Microsoft licensing agreement at no additional cost.

With Intune, you can:

- Set rules and configure settings on personal and organization-owned devices to access data and networks.
- Deploy and authenticate apps on devices -- on-premises and mobile.
- Protect your company information by controlling the way users access and share information.
- Be sure devices and apps are compliant with your security requirements.

Security Function: Protect

The maturity level based on the 28 IG FISMA Metrics questions for the "Protect" function is Level 2 (Defined), Not Effective.

4. CNCS Must Implement Standard Baseline Configurations

Recommendation 4: Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations. (New)

AmeriCorps Response: AmeriCorps concurs. AmeriCorps has finished configuring Nessus to scan for baseline configurations.

Recommendation 5: Fully implement standard baseline configurations for all platforms in the CNCS information technology environment and establish processes to test and monitor for compliance with established CNCS security standards. (Modified Repeat)

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

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

Management stated that the removal of mandatory enforcement of PIV authentication was a technical change to allow uninterrupted telework access in the event a user had PIV-related issues during to the COVID-19 pandemic. Management was concerned that users would not be able to obtain a new PIV card should their card become damaged or lost since most personnel were working remotely. Management stated that in order to lessen the downtime for users, it would be faster for the help desk personnel to advise the user to log in with their network password rather than modifying the laptop settings to disable PIV requirements on a case-by-case basis. Management believed that most users would continue to use their PIV cards as staff were not advised of the change unless they reached out to the help desk because of a problem.

Recommendation 6: Assess and document a plan for reinstating mandatory enforcement of multifactor authentication as recommended by the Cybersecurity and Infrastructure Security Agency (CISA) to address increased risks with the large number of personnel teleworking during the pandemic. (New)

AmeriCorps Response: AmeriCorps concurs. Management responses are captured above.

6. CNCS Must Strengthen Account Management Controls

Recommendation 7: AmeriCorps will ensure Momentum Help Desk system administrators validate user accounts are approved prior to granting Momentum access. (New)

AmeriCorps Response: AmeriCorps concurs with this finding. AmeriCorps will implement the suggested process.

Recommendation 8: Ensure that accounts for users that never logged in are included in the AmeriCorps Inactive script. (New)

AmeriCorps Response: AmeriCorps concurs with this finding. AmeriCorps will implement the suggested process

7. AmeriCorps Must Ensure Role-based Privacy Training Is Conducted Annually

Recommendation 9: Ensure all personnel whose responsibilities include access to PII complete annual privacy-role based training. (New)

AmeriCorps non-concurs: All users who access PII fall into the general user category and are required to take privacy training annually which is included as part of the annual cybersecurity training. There are some people who handle PII more than others, however they are not serving in a specific privacy role. AmeriCorps has pro-actively given these people additional PII training in May 2019 and they will receive further training in the future. There is no requirement for these people to receive this additional training annually as the report indicates.

The Privacy Specialist (Aaron Goldstein) is trained annually as part of his privacy certifications. He holds the following certification

- Certified Information Privacy Manager (CIPM)
- Certified Information Privacy Professional/U.S. Government (CIPP/G)
- Fellow of Information Privacy (FIP)

To retain the CIPM he must complete 20 hours of privacy training every two years.

Security Function: Detect

The maturity level based on the five IG FISMA Metric questions for the "Detect" function is Level 1 (*Ad-Hoc*) or Not Effective.

Security Function: Respond

CLA's assessment did not find any weaknesses for controls evaluated in the "Respond" function.

Security Function: Recover

CLS's assessment did not find any weaknesses for controls evaluated in the "Recover" function.

OFFICE OF INSPECTOR GENERAL

CORPORATION FOR
NATIONAL & COMMUNITY SERVICE

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

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