AmeriCorps

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2021 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF AMERICORPS

FINAL AUDIT REPORT

NUMBER: OIG-EV-22-03

DECEMBER 15, 2021

OFFICE OF INSPECTOR GENERAL
AmeriCorps

OFFICE OF INSPECTOR GENERAL
AmeriCorps

December 15, 2021

MEMORANDUM TO: Pape Cissé
Chief Information Officer

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

SUBJECT: Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of AmeriCorps (OIG Report- EV-22-03)

Enclosed is the final report on the Fiscal Year 2021 Federal Information Security Modernization Act (FISMA) Evaluation of AmeriCorps, the Office of Inspector General's (OIG) Report EV-22-03. AmeriCorps' OIG contracted with the independent certified public accounting firm of CliftonLarsonAllen LLP (CLA) to conduct the FISMA evaluation for Fiscal Year (FY) 2021. CLA is responsible for the attached final report. We reviewed CLA's report and related documentation and inquired of its representatives. Our review was not intended to enable us to express, and we do not express, an opinion on the matters contained in the final report. Our review disclosed no instances where CLA did not comply with the *Quality Standards for Inspections and Evaluations* issued by the Council of Inspectors General on Integrity and Efficiency.

If you have any questions or wish to discuss the draft report, please contact me at (202) 875-0245 or m.colter@americorpsoig.gov.

cc: Malcom Coles, Acting Chief Executive Officer
Jenny Mauk, Chief of Staff
Gina Cross, Chief Operating Officer
Syed Murshed, Deputy Chief Information Officer
Bilal Razzaq, Chief Information Security Officer
Fernando Laguarda, General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits and Investigations Program Manager
Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

AmeriCorps
Federal Information Security Modernization Act Evaluation

Fiscal Year 2021

December 13, 2021

Final Report

A member of Nexia International

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. AmeriCorps'[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) 2021. The objective was to determine the effectiveness of AmeriCorps' information security program 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 nine IG FISMA Metric Domains and five Function areas.[3]

AmeriCorps relies on IT systems to accomplish its mission of making grants and managing a residential national service program. AmeriCorps' cybersecurity program must protect these systems from malicious attacks and other compromises that may put its sensitive information, including personally identifiable information (PII), or taxpayer dollars at risk.

We have determined that AmeriCorps' 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 maturity scale.[4]

Overall, AmeriCorps has made little progress in maturing its information security program since FYs 2018, 2019, and 2020. See Table 1 below, comparing AmeriCorps' FY 2021 maturity scores by security function with those of FYs 2018, 2019, and 2020.[5] Most of the maturity metrics remain unchanged from prior years. Specifically, since FY 2020, AmeriCorps advanced in only one of the function areas, Detect, remaining at the same level in the other four function areas.

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

[2] Effective on October 15, 2020, the operating name of the agency was changed from Corporation for National and Community Service to AmeriCorps.

[3] The FY 2021 IG FISMA Reporting 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.

[5] For FY 2021, a new domain—Supply Chain Risk Management (SCRM)—was added to the Identify function area, but it is not included this year in rating the Identify function.

Table 1: Comparison of Maturity Ratings by Function in FYs 2018 -- 2021

Security Function[6]	Maturity Level FY 2018	Maturity Level FY 2019	Maturity Level FY 2020	Maturity Level FY 2021
Identify	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)	Defined (Level 2)
Protect	Defined[7] (Level 2)	Defined[8] (Level 2) – *Assessed Rating*[9]	Defined[10] (Level 2)	Defined[11] (Level 2)
Detect	Defined (Level 2)	Ad Hoc (Level 1)	Ad Hoc (Level 1)	Defined (Level 2)
Respond	Consistently Implemented (Level 3)	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)	Consistently Implemented (Level 3)
Overall	**Not Effective**	**Not Effective**	**Not Effective**	**Not Effective**

Consistent implementation of an information security program and monitoring of security controls remain challenges for AmeriCorps. The agency lacks an overall strategy for improving IT security to an effective level and the accountability structure necessary to reach that result. **(Finding 1)**. We note that AmeriCorps did not have a permanent Chief Information Security Officer (CISO), the position primarily responsible for information security, as required by the FISMA Act, from October 2020 to June 2021.

AmeriCorps has not made significant progress in implementing prior recommendations, some dating back to 2017. Since last year, the agency demonstrated actions to resolve eight of the 39 open recommendations from the FY 2017 – FY 2020 FISMA evaluations, yielding slight improvements in IG FISMA Metrics results. Implementing more of these recommendations will help AmeriCorps to mature its information security program and bring it closer to effectiveness. See **Appendix III** for the status of prior year recommendations.

[6] See Appendix I Table 2 and Table 3 for definitions and explanations of the Cybersecurity Framework Security Functions and Metric Domains.

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

[8] Ibid 7.

[9] For FY 2019, the auditors assessed the Protect function's maturity level as Defined (Level 2), although the performance metrics yielded a calculated score of Managed and Measurable (Level 4), stemming from its security training. The auditors concluded that the severity of control weaknesses in the other components of the Protect function--configuration management, identity and access management, and data protection and privacy, outweighed the strength of security training, because they leave AmeriCorps' systems vulnerable to unauthorized access, loss of personally identifiable information and disruption. The scoring methodology allows auditors to make judgments in the case of such anomalies.

[10] Ibid 7.

[11] Ibid 7.

The control weaknesses that continue to prevent AmeriCorps from maturing its cybersecurity program relate to the following DHS IG metrics:

- Organization-wide risk management strategy,
- IT asset inventory management,
- 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 remains at the *Defined* maturity level this year because the organization-wide risk management strategy is still not fully implemented, and control weaknesses remain with IT asset inventory and mobile device management.

   Specifically, the risk register developed to record identified risks at the mission and business process level, Tier 2 as defined by the NIST, was outdated and therefore did not reflect risks of the current environment. AmeriCorps management attributed the delay in updating the risk register to significant turnover in the Office of the Chief Risk Officer in FY 2020, including the Chief Risk Officer and focusing on risks the agency faced due to the COVID pandemic.

   The tracking of information technology components in the asset inventory was incomplete, and software assurance controls have not been fully implemented for mobile devices due to delays in implementing a new mobile device management tool. These control weaknesses affect four of the 10 metrics in the risk management domain. Completing the updated Tier 2 risk register, properly managing the IT asset inventory, and implementing the new mobile device management tool will assist AmeriCorps in improving the Identify function above the *Defined* maturity level.

2. The **Protect** function also remains at the *Defined* maturity level this year because of the issues related to PIV multifactor authentication, standard baseline configurations, and vulnerability management.

   AmeriCorps continues to refrain from enforcing PIV multifactor authentication for all users, leading to a low score in the domain of identity and access management. Agency management attributes this to the need for full-time telework during the COVID-19 pandemic. As we pointed out last year, that conflicts with government-wide guidance issued by the Cybersecurity and Infrastructure Security Agency (CISA) directing agencies to use multifactor authentication during pandemic-related telework. This control weakness affects four of the eight metrics in this domain.

The maturity level for the configuration management domain remains at the *Defined* maturity level because standard baseline configurations are not fully implemented, and vulnerability and patch management controls are not consistently employed. These control weaknesses affected five of the eight metrics in this domain.

The most effective way for AmeriCorps to improve its maturity level in the Protect function is to reinstate mandatory enforcement of PIV multifactor authentication, fully implement standard baseline configurations, and strengthen vulnerability and patch management controls.

3. The **Detect** function area is *Defined* because AmeriCorps does not consistently remediate vulnerabilities on the schedule required by its *Cybersecurity Information Security Continuous Monitoring Strategy (ISCM).* In addition, AmeriCorps does not consistently implement the change management, configuration management and asset management components of the ISCM Strategy.

   Furthermore, the lack of a Tier 2 risk register inhibits the ability of AmeriCorps to address IT risks at the organization and business process level in the ISCM Strategy. Finally, AmeriCorps has not identified and defined performance measures for assessing the effectiveness of the ISCM program. These control weaknesses affected three of the four metrics in the continuous monitoring domain.

In addition, the **Respond** and **Recover** function areas are *Consistently Implemented* and therefore not effective. AmeriCorps did not conduct incident response testing and does not analyze performance measures to monitor the effectiveness of its overall incident response capability. In addition, AmeriCorps did not perform a disaster recover test for two key systems and does not collect and integrate metrics on the effectiveness of its information system recovery and contingency planning activities to provide continuous situational awareness across the organization.

Focusing on these controls is key to AmeriCorps increasing all function areas to an effective maturity level. To address the continuing weaknesses in AmeriCorps' information security program and practices, we have added 13 new recommendations to the 31 unimplemented recommendations from prior years. Implementing these recommendations will assist AmeriCorps in addressing challenges in its development of a mature and effective information security program.

Management's Response and Evaluator's Comments

In response to the draft report, AmeriCorps concurred with 12 of the 13 new recommendations, but it did not provide target dates of implementation for 10 and corrective actions and a target date of implementation for one of the 12 recommendations. We advise that AmeriCorps develop

corrective action plans to include target completion dates for each recommendation, so that its progress can be tracked and reported in the FY 2022 FISMA evaluation.

With respect to Recommendation 13, AmeriCorps did not concur to establish an oversight process to ensure that the disaster recovery plan is tested for the General Support System (GSS) and Electronic-Systems for Program Agreements and National Service Participants (eSPAN), and associated training is conducted on an annual basis. AmeriCorps stated that they combine incident response and disaster recovery testing for these systems and therefore this recommendation is duplicative with Recommendation 12.

Recommendation 12 addresses performing an annual incident response test or exercise in accordance with AmeriCorps' policies and is not duplicative of Recommendation 13; NIST considers incident response testing and disaster recovery testing as separate controls. According to NIST, incident response testing evaluates the handling capability for security incidents that includes preparation, detection and analysis, containment, eradication, and recovery. In addition, NIST describes contingency plan (disaster recovery) testing as addressing both information system restoration and implementation of alternative mission/business processes when systems are compromised. Provided the combined test that AmeriCorps plans to complete addresses both the NIST requirement for incident response and disaster recovery testing, we agree with management's plan.

In addition, AmeriCorps stated that 16 of the 28 recommendations from the prior year have been closed by AmeriCorps but remain open after CLA determined there was insufficient evidence to close them. AmeriCorps stated they are in the process of reviewing those 16 to determine what additional remediations need to be addressed. AmeriCorps acknowledges the other 12 recommendations are open and stated they are on schedule to be remediated. We recognize that AmeriCorps documented correction action plans for the open prior year recommendations.

AmeriCorps' comments are included in their entirety in Appendix IV.

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

CLIFTONLARSONALLEN LLP

Arlington, VA
December 13, 2021

FISMA EVALUATION FINDINGS

IT Governance Strategic Vision

1. AmeriCorps Must Develop and Implement a Strategy, Including Enforcing Accountability within OIT, for Improving its Information Security Program to an Effective Level

Information technology is the backbone of AmeriCorps' operations; the agency cannot achieve its mission without reliable data and information systems. Nevertheless, AmeriCorps' information technology program remains stagnant at an overall rating of *Defined*, far short of the Managed and Measurable standard needed to be considered effective. At its current level, AmeriCorps' core business is vulnerable to disruption, unauthorized access, malicious attacks, and improper disclosure of sensitive information. The agency has made little progress towards improving its information security since 2017.

The agency lacks an overall strategy for improving IT security to an effective level and the accountability structure necessary to reach that result. The FY 2018[12] and 2019[13] FISMA evaluation reports included recommendations for AmeriCorps to analyze the IG FISMA Metrics related to each security function and develop a multi-year strategy of corrective actions that would achieve measurable improvement. In FY 2020, AmeriCorps reported that it had completed a gap analysis and identified the corrective actions required to improve security controls in each of the function areas. However, only two of the corrective action plans made available to evaluators contemplated achieving effectiveness as measured by the IG Metrics. Moreover, the plans did not lead to demonstrable progress. Consequently, 31 prior year recommendations remain open.

Simply put, AmeriCorps does not consistently enforce its cybersecurity program, has not followed Federal guidance on IT security during telework, and has not implemented prior year evaluation recommendations. Overall, the IT security program suffers from a lack of leadership, management support, and accountability. Although the FISMA legislation requires each agency to have a Chief Information Security Officer (CISO), whose principal duty is cybersecurity, AmeriCorps allowed this position to remain vacant from October 2020 to June 2021, with an acting official in the role. Given the agency's weaknesses in key information security controls and the importance of this function, the lack of a permanent CISO, with the ability to advise the agency head on key issues of cybersecurity policy, enforcement and needed improvements, detracted from the opportunity to make progress. Now, the agency is required to scale up programmatically at the same time that it must grapple with weaknesses in information security.

[12] Recommendations 7, 21, 23, 24, and 25, *Fiscal Year 2018 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 18, 27, 29, 30, and 31, (OIG Report No. 19-03, March 1, 2019). During the FY 2020 FISMA evaluation, we closed the FY 2018 recommendations because they were superseded by the FY 2019 recommendation.

[13] Recommendations 9, 29, 31, 32, and 33 *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 14, 27, 29, 30 and 31 (OIG Report No. 20-03, January 24, 2020).

AmeriCorps' CISO is also responsible for implementing AmeriCorps' privacy program. The FY 2020 FISMA evaluation report[14] included a recommendation to ensure that all personnel whose responsibilities include access to PII complete annual privacy-role based training. For the second year in a row, our evaluation found that AmeriCorps did not conduct annual role-based training, which the agency attributes to the departure of the prior CISO and the Privacy Program Analyst. It is not clear why the Acting CISO did not undertake the necessary training or why the Chief Information Officer (CIO), to whom the CISO reports, did not ensure fulfillment of that responsibility.

The CISO's office requires consistent support from the agency's leadership in developing and implementing a strategy to achieve an effective level of information security at AmeriCorps. This includes ensuring accountability within OIT leadership for accomplishing milestones and achieving measurable results.

We recommend the AmeriCorps Acting Chief Executive Officer:

> ***Recommendation 1:*** Design and implement an effective accountability system that includes clear expectations of goals, performance measures, estimated target dates, and monitoring to hold OIT leadership accountable for improving AmeriCorps' information security program to an effective level. *(New)*

[14] Recommendation 9, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 20, (OIG Report No. 21-03, December 18, 2020).

Security Function: Identify

2. AmeriCorps Must Improve Its Inventory Management Process

FY 2021 IG FISMA Metric Area: *Risk Management*

Federal agencies are required 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.[15] In addition, the agency's internal policy, the *AmeriCorps Cybersecurity Control Families* document, requires the information system component inventory to be reviewed and updated at least annually.

AmeriCorps did not maintain proper inventory management controls. Reviewing the inventory listing of 3,436 IT assets, we found the following gaps in critical information:

- Location was not documented for 377 deployed assets;
- Primary client (owner) was not documented for 279 assets;
- Serial number was not documented for 61 assets; and
- Asset number was not documented for 91 assets.

This error rate demonstrates that the quality control process for the asset inventory was not adequate. Although AmeriCorps management stated that the AmeriCorps Tier 2 support team updated the inventory information, they did not complete and update all of the fields specified in The AmeriCorps *Standard Operating Procedures* (*SOP) Asset Tracking Procedures*, Version 2.8, when moving items in and out of storage at the AmeriCorps Headquarters (HQ) location. Management also stated that the Tier 2 Support Lead will provide refresher training on the *Asset Tracking Procedures* and institute a spot check to ensure they are following the established procedures to remedy this issue.

The AmeriCorps *SOP Asset Tracking Procedures, Version 2.8*, states the following requirements regarding AmeriCorps hardware inventory management:

> Remedyforce Configuration Management Database (CMDB) assets must have the following fields completed when new assets are added to the information system: Asset Number, Primary Client, Instance Name, Name/Description, Serial Number, Configuration Item Status (deployed or in storage), Operational Status, Location, and Purchase Order Number.

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

[15] NIST Special Publication (SP) 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control CM-8, Information System Component Inventory, page F-73.

The FY 2019 FISMA evaluation report[16] included the following recommendations to assist AmeriCorps 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 that corrective action on these recommendations was completed. However, we requested, but did not receive, sufficient evidence to validate the implementation of these recommendations. Therefore, these recommendations remain open.

The FY 2020 FISMA evaluation report[17] also included a recommendation to perform and document an oversight process to ensure physical inventory reviews and updates are fully documented to include the exact location of all IT assets. Management did not implement this recommendation, which we are superseding with Recommendation 3, below.

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

> ***Recommendation 2:*** Complete asset tracking refresher training for the Tier 2 support team. *(New)*
>
> ***Recommendation 3:*** Update the AmeriCorps SOP Asset Tracking Procedures to include a quality control process for the Tier 2 Lead to review the IT asset inventory to ensure the required fields for the IT assets are documented; and implement the new process. *(New)*

3. AmeriCorps Must Maintain Current Interconnection Security Agreements

FY 2021 IG FISMA Metric Area: *Risk Management*

Federal agencies that share data with other Federal agencies must document the technical and security requirements of their information interchange via ISAs.[18] The ISA between AmeriCorps and the Social Security Administration expired in November 2018, having been signed in November 2015. The *AmeriCorps Cybersecurity Control Families* document makes AmeriCorps' Information System Security Officer (ISSO) responsible for ensuring that connections from other information systems are authorized through the use of ISAs and reviewing and updating ISAs

[16] 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).

[17] Recommendation 1, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 10, (OIG Report No. 20-03, January 24, 2020).

[18] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control CA-3, System Interconnections, page F-57.

annually. Management acknowledged the error and characterized it as an oversight. Management further stated that a draft document dated April 28, 2021, is under review and will be submitted to SSA for signature.

Without an executed ISA, AmeriCorps is not guaranteed appropriate security controls for the interconnection and the interconnected systems, and the process for confirming the continued operating effectiveness of those security controls is not established. Security control weaknesses increase the risk of compromising the confidentiality, integrity, and availability of the data the interconnected systems store, process, or transmit. The lack of an ISA places at risk the large volume of Personally Identifiable Information shared between AmeriCorps and SSA.

To assist AmeriCorps in strengthening the management of system interconnections, we recommend that AmeriCorps:

> ***Recommendation 4:*** Complete and execute the ISA with the Social Security Administration. *(New)*
>
> ***Recommendation 5:*** Document and implement an annual review process to validate that all agreements for system interconnections are kept current. *(New)*

4. AmeriCorps Must Develop a Supply Chain Risk Management Strategy and Related Policies and Procedures

FY 2021 IG FISMA Metric Area: *Supply Chain Risk Management*

AmeriCorps did not develop, document, and communicate an overall SCRM strategy, implementation plan, and related policies and procedures to guide and govern supply chain risk management activities. According to NIST, supply chain risks may include for example, introduction of counterfeit or tampering of IT components, insertion of malicious software and hardware, and inferior manufacturing and development practices in the Information and Communication Technology (ICT) supply chain.[19]

Management stated that AmeriCorps purchases all hardware through government approved vehicles, most specifically General Services Administration (GSA) Schedule/GSA Advantage, and all items are vetted for proper supply chain approaches. Management further stated that AmeriCorps does not purchase hardware directly from manufacturers. However, management has not documented this practice or issued a written SCRM Strategy, implementation plan, and related policy and procedures due to other unspecified higher priority tasks. Accordingly, nothing prevents the agency from deviating from its practice of relying on GSA for purchases of information technology.

[19] NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, page 1.

Public law 115-390 – 115th Congress, Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act or the ‘‘SECURE Technology Act” (December 21, 2018) states:

§1326 (a). Requirements for executive agencies

‘‘(a) IN GENERAL.—The head of each executive agency shall be responsible for—
‘‘(1) assessing the supply chain risk posed by the acquisition and use of covered articles and avoiding, mitigating, accepting, or transferring that risk, as appropriate and consistent with the standards, guidelines, and practices identified by the Council under section 1323(a)(1); and ‘‘(2) prioritizing supply chain risk assessments conducted under paragraph (1) based on the criticality of the mission, system, component, service, or asset. ‘‘

(b) INCLUSIONS.—The responsibility for assessing supply chain risk described in subsection (a) includes— ‘‘(1) developing an overall supply chain risk management strategy and implementation plan and policies and processes to guide and govern supply chain risk management activities;

NIST SP 800-161, *Supply Chain Risk Management Practices for Federal Information Systems and Organizations*, Chapter 2, section 2.2.1 FRAME, states:

An organization Information and Communication Technology SCRM policy is a critical vehicle for guiding ICT SCRM activities. Driven by applicable laws and regulations, this policy should support applicable organization policies including acquisition and procurement, information security, quality, and supply chain and logistics. It should address goals and objectives articulated in the overall agency strategic plan, as well as specific mission functions and business goals, along with the internal and external customer requirements. It should also define the integration points for ICT SCRM with the agency’s Risk Management Process and System Development Life Cycle.

Without the development of an SCRM strategy, implementation plan, and related policies and procedures, AmeriCorps may deviate from its practice of relying on GSA for IT purchases and therefore be exposed to unanticipated, and therefore unmitigated, supply chain risks.

To assist AmeriCorps in strengthening its supply chain risk management processes, we recommend that AmeriCorps:

> ***Recommendation 6:*** Develop, document, and communicate an overall SCRM strategy, implementation plan, and related policies and procedures to guide and govern supply chain risk management activities. If AmeriCorps intends to limit its IT purchases to GSA vendors, it should so state, and indicate who, if anyone, must approve exceptions. *(New)*

Security Function: Identify
Maturity Model Scoring

The maturity level based on the 14 IG FISMA Metrics for the "Identify" function is Level 2 (*Defined*), Not Effective, as depicted in the chart below:[20]

Function	Count	IG FISMA Metrics
Ad Hoc (Level 1)	4	12, 13, 14, and 15[21]
Defined (Level 2)	5	2, 5, 6, 7, and 10
Consistently Implemented (Level 3)	2	3 and 9
Managed and Measurable (Level 4)	2	1 and 8
Optimized (Level 5)	1	4
Calculated Maturity Level: Defined (Level 2), Not Effective		

[20] Ratings depend on the most frequent rating in the function or domain, rather than on an average.

[21] Metrics 12-15 are from the Supply Chain Risk Management domain. The FY 2021 IG FISMA Reporting Metrics indicated that to provide agencies with sufficient time to fully implement NIST SP 800-53, Revision 5, in accordance with OMB A-130, these new metrics should not be considered for the purposes of the Identify framework function rating, and therefore would not be factored into the overall rating.

Security Function: Protect

5. AmeriCorps Must Improve its Vulnerability and Patch Management Controls

FY 2021 IG FISMA Metric Area: *Configuration 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. At AmeriCorps, the ISSO is responsible for remediating these and other vulnerabilities on a set schedule. Our vulnerability scans found that the total number of critical and high-severity vulnerabilities has decreased by 75 percent, representing substantial progress. (**Figure 1**). Still, AmeriCorps' network remains vulnerable at the critical and high-severity levels due to unpatched software, improper configuration settings, and unsupported software.

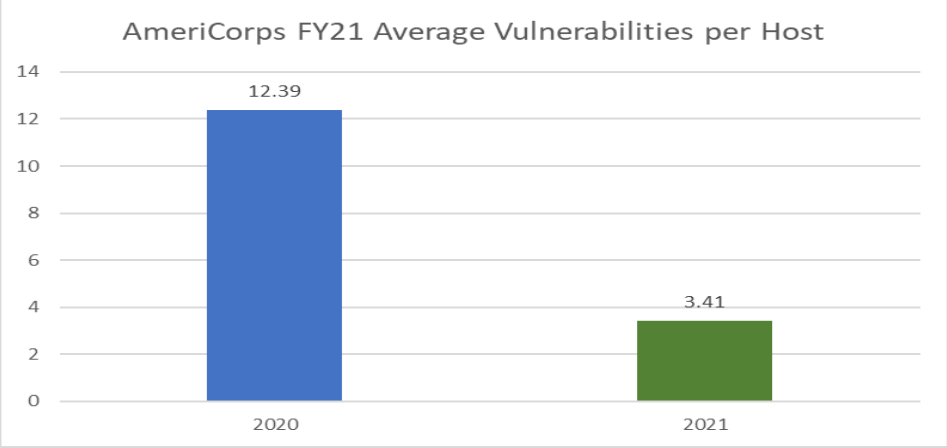


Figure 1. Comparison of the total number of critical and high-risk vulnerabilities identified by the independent auditors' credentialed vulnerability scans, averaged by information system from FY 2020 and 2021.

Further, using the vulnerability scoring system provided by Tenable Nessus,[22] AmeriCorps did not resolve critical vulnerabilities within seven days of occurrence and high-risk vulnerabilities within 30 days, as required by its internal operating policies. AmeriCorps still has not resolved the configuration weaknesses including Secure Sockets Layer (SSL) 2.0 and 3.0 with cryptographic

[22] The mission of the Common Vulnerability Scoring System (CVSS) is based upon the Common Vulnerabilities and Exposures (CVE®) Program used to identify, define, and catalog publicly disclosed cybersecurity vulnerabilities. There is one CVE Record for each vulnerability in the catalog. The vulnerabilities are discovered, then assigned and published by organizations from around the world that have partnered with the CVE Program. Partners publish CVE Records to communicate consistent descriptions of vulnerabilities. IT and cybersecurity professionals use CVE Records to ensure they are discussing the same issue, and to coordinate their efforts to prioritize and address the vulnerabilities. The CVE Records as assigned a CVSS score which is used by Nessus to assign the Severity Risk.

flaws,[23] Simple Network Management Protocol (SNMP) Default community strings,[24] OpenSSH flaw eliminating brute-force password protections,[25] and Intelligent Platform Management Interface (IPMI) password hash disclosures[26] from credential and non-credential scans that were published before calendar year 2020.

Specifically, we noted patch management issues at the AmeriCorps HQ, Washington, DC:

- Our non-credential[27] scan of 743 systems at AmeriCorps HQ found **565 total critical and high-risk vulnerabilities** (131 critical and 434 high-risk) related to patch management, configuration management, and unsupported software. Of the total, 255 were caused by missing patches, 215 were caused by configuration weaknesses, and 95 were caused by unsupported software.
- Our scan of 73 Windows systems, including servers and workstations, identified **85 critical and 164 high-risk vulnerabilities** arising from inadequate patch management, configuration management, and unsupported software.[28] Of the 249 total critical and high-risk vulnerabilities, 97 were caused by missing patches, 51 were caused by configuration weaknesses, and 101 were caused by unsupported software. **Figures 2 and 3** depict AmeriCorps HQ vulnerabilities by criticality and type.

  The 101 vulnerabilities due to unsupported software before and during 2020, relate to the following:

  - VMware ESX / ESXi version 6.0 unsupported as of March 12, 2020
  - VMware ESX version 4.1 unsupported as of May 21, 2014
  - Web servers Microsoft Internet Information Services 7.5 unsupported on January 14, 2020
  - Windows operating system Server 2008 R2 unsupported on January 14, 2020
  - Oracle Database version 11.2.0.3.0 unsupported on December 31, 2020
  - Microsoft SQL server 2008 version 10.0.6556.0 unsupported on July 9, 2019

[23] The server accepts connections using SSL 2.0 and/or SSL 3.0. These versions use exploitable CBC ciphers or security session negotiation flaws which allow an attacker to decrypt protected communications.

[24] SNMP uses the default password to protect sensitive configuration information.

[25] The SSL server has a configuration flaw which ignores the normal restriction of 6 failed login attempts which would normally reset the connection. This flaw allows the attacker to brute force username and password attempts without limit.

[26] The IPMI protocol is affected by an information disclosure vulnerability whereby a remote attacker can obtain password hash information for valid user accounts.

[27] We performed two separate Nessus vulnerability scans – credential and noncredential scans. The credential scans are performed with a privileged account contrasted to noncredential scans which use default system and application passwords. Credential scans dig deeper into application and operating system vulnerabilities while noncredential scans report vulnerabilities exposed to the network by looking only at network services from an outsider.

[28] We tried but were unable to scan an additional 29 Windows systems due to credentialing issues.

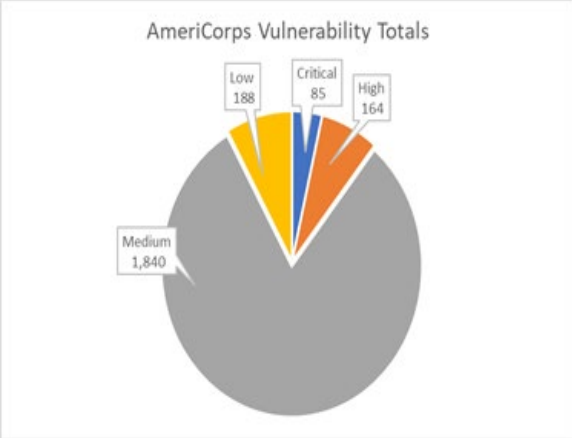


Figure 2 HQ total vulnerabilities by criticality from credentialed scans

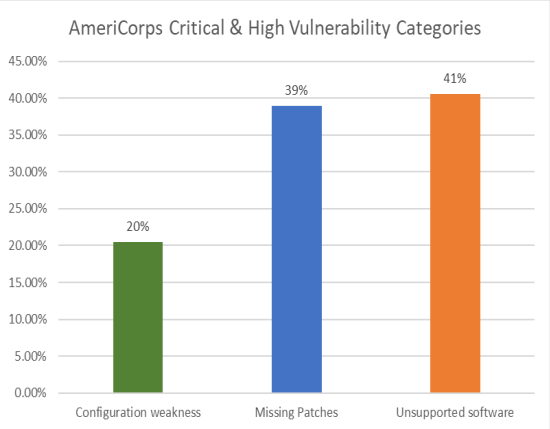


Figure 3 HQ total vulnerabilities by type from credentialed scans

- Our non-credential scans, found 565 critical and high-risk vulnerabilities, (99 percent of which were from 2020 or before). Our credential scans found that 80 percent of the 249 critical and high-risk vulnerabilities were from 2020 or before. **Figure 4** depicts the distribution of vulnerability ages.

  Information regarding each of the above configuration weaknesses[29] was made public during and before 2020. They related to unprotected file shares, Windows services, IPMI authentication disclosures, weak encryption protocols, and SNMP default community names.

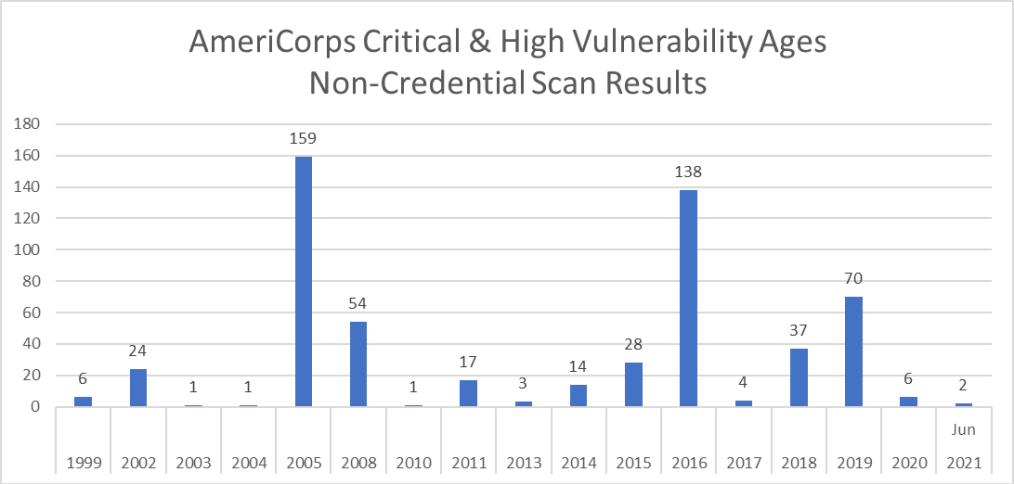


Figure 4 HQ vulnerability ages from non-credentialed scans

[29] 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.

The overall deployment of vendor patches and system upgrades to mitigate the vulnerabilities continues to be inconsistent and not effective for the AmeriCorps HQ network. AmeriCorps had no process in place to ensure the timely correction of identified flaws, such as configuration weaknesses or unsupported software. We note, however, that AmeriCorps is keeping current on Microsoft patching.

The *AmeriCorps Cybersecurity Control Families* document states that the ISSO is responsible for:

- Scanning for vulnerabilities in the information system and hosted applications at least monthly and when new vulnerabilities potentially affecting the system/applications are identified and reported; and
- 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.

AmeriCorps HQ's information systems face elevated risk from the failure to apply available patches. A malicious actor, using unsophisticated techniques could take control of systems, to cause a denial-of-service attack or to allow unauthorized access to the AmeriCorps HQ systems and applications. The risks are exacerbated when an agency relies on software that the vendor no longer supports, which leaves security weaknesses unfixed, exposing those systems to increased attack methods compromising the confidentiality, integrity, and availability of data.

The FY 2019 FISMA evaluation report[30] included recommendations to assist AmeriCorps in improving their vulnerability management program. These recommendations included implementing a process to track patching of network devices and servers by the defined risk-based patch timelines in AmeriCorps policy; replacing information system components when support is no longer available; 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 AmeriCorps improved current patching since last year, issues remain with applying older patches and remediating older configuration weaknesses. Patches remain missing from as far back as 2013, and some configuration weaknesses date back to 1999. Based on the results of our independent scans, we note that management did not take corrective action on these recommendations. The FY 2019 recommendations remain open, and we are not making additional recommendations at this time.

[30] 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).

6. AmeriCorps Must Implement Standard Baseline Configurations

FY 2021 IG FISMA Metric Area: *Configuration Management*

Standard baseline configurations are security settings applied to information systems to decrease the risk of vulnerabilities being exploited. AmeriCorps did not develop baseline configuration documentation for all information system components. Specifically, AmeriCorps did not document standard baseline configurations for Microsoft SQL Server 2008 and Windows Server 2008 R2 until August 2021, after notification by CLA of the missing baselines.

Management stated that baselines for systems that are being decommissioned or upgraded to newer versions were assigned lower priorities. Management also stated they did not address baselines for Microsoft SQL Server 2008 and Windows Server 2008 R2 until recently, due to efforts being directed to unspecified higher priority operational tasks.

The *AmeriCorps Cybersecurity Control Families* document requires the ISSO to establish, document, and implement baseline configuration settings for the IT components employed within the information system, and monitor and control changes to the configuration settings. Additionally, the ISSO is responsible for identifying and documenting exceptions from established configuration settings for individual components within the information system based on explicit operational requirements.

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

The FY 2019[31] and FY 2020[32] FISMA evaluation reports made recommendations for AmeriCorps to establish and document standard baseline configurations for all platforms in the AmeriCorps IT environment and to ensure that these standard baseline configurations were appropriately implemented, tested, and monitored for compliance with established AmeriCorps security standards. This includes documenting the business justification for any approved deviations from the configuration baselines. The FY 2019 and 2020 recommendations remain open, and we are not making additional recommendations related to baseline configuration controls.

[31] Recommendation 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).

[32] Recommendations 4 and 5, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 17, (OIG Report No. 21-03, December 18, 2020).

7. AmeriCorps Must Properly Document the Security Impact Analysis for Information System Changes

FY 2021 IG FISMA Metric Area: *Configuration Management*

Before implementing any IT system changes, an agency's personnel with information security responsibilities (e.g., Information System Administrators, Information System Security Officers, Information System Security Managers, and Information System Security Engineers) are required to consider their potential security implications.[33]

AmeriCorps' *Cybersecurity: Security Impact Analysis SOP,* Version 2.0, requires the completion of a SIA questionnaire in order to determine and document whether a SIA is needed for each change implemented.

We were not able to validate whether a SIA was needed for 13 GSS changes, three eSPAN system changes, and two Momentum system changes selected for testing. AmeriCorps assured us that they completed the questionnaires necessary to make this determination, but they did not maintain the questionnaires and could not provide evidence to support their conclusions that no SIA was required. AmeriCorps' SIA SOP does not explicitly require retention of the questionnaires, uploading them to the change management tool, or other electronic storage. Without the questionnaires, a third party cannot validate completion of this essential step or determine whether the responses support management's actions or omissions.

Without assessing risk for information system changes, security deficiencies and vulnerabilities may exist and go undetected. This may increase the exposure of AmeriCorps' systems to potential threats and attacks.

To assist AmeriCorps in continuing to strengthen the change management program, we recommend that AmeriCorps:

> ***Recommendation 7:*** Update the SIA SOP to require maintaining completed SIA questionnaires in the change management tool for all system changes for validating whether each configuration change requires a SIA. *(New)*

[33] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control CM-4, Security Impact Analysis, page F-68.

8. AmeriCorps Must Enforce Multifactor Authentication for Information System Users

FY 2021 IG FISMA Metric Area: *Identity and Access Management*

Federal information systems are required to uniquely identify and authenticate users prior to granting access.[34] 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, 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."

AmeriCorps removed mandatory enforcement of PIV authentication in March 2020 in response to the COVID-19 pandemic. This was contrary to the recommendation of Cybersecurity and Infrastructure Security Agency (CISA) alert AA20-073A, March 13, 2020, that, agencies require multifactor authentication for all users, precisely because of the increased risks associated with widescale telework across the Federal government. AmeriCorps reached its original decision to suspend enforcement of PIV authentication without conducting and documenting a risk assessment or formally accepting the associated risks. After we brought this issue to AmeriCorps' attention, management issued a Risk Acceptance Memorandum in June 2020, in effect for a ninety day period. Management thereafter allowed the Risk Acceptance Memorandum to expire and did not issue a new memorandum until July 2021, when prompted by our questions in connection with this evaluation. Management's rationale for suspending multifactor authentication consisted of predictions about the likely burden of enforcing PIV authentication, without any data, testing, or piloting.

Management stated that, despite last year's recommendation and the guidance from CISA, it did not reinstate PIV enforcement because the majority of the AmeriCorps' workforce continued to telework during FY 2021 due to the COVID-19 pandemic. Management also stated that PIV enforcement will be re-enabled once all personnel have returned to work in AmeriCorps offices which is tentatively scheduled for January 4, 2022. However, given the Federal policy in favor of expanded telework even after January 4, 2022, AmeriCorps may have to address security for remote work well into the future.

The lack of multifactor authentication in place during extended periods of telework markedly increases the risk of unauthorized access. The more time available to malicious actors to gain information about AmeriCorps' users and systems, the greater the likelihood/risk that they will obtain unauthorized access. In addition, without multifactor authentication, there is an

[34] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control IA-2, Identification and Authentication (Organizational Users), page F-90.

increased risk that security controls, such as firewalls and malicious code/program detection software, can be bypassed, allowing access to sensitive AmeriCorps information.

As a result, AmeriCorps' information systems are at increased risk for disruption of operations and loss of productivity, plus unauthorized access to and disclosure of sensitive information, including PII which may result in personal harm, loss of public trust, legal liability or increased costs of responding to a breach. Ultimately, AmeriCorps' current information system environment will require strong cybersecurity measures to remediate the heightened risks and safeguard assets against potential security threats.

In addition to the FY 2020 recommendation, to assist AmeriCorps in complying with CISA's recommendation regarding strong authentication controls during widescale telework across the Federal Government, we recommend that AmeriCorps management:

> ***Recommendation 8:*** Immediately reinstate mandatory enforcement of multifactor authentication in accordance with CISA's recommendation. *(New)*
>
> ***Recommendation 9:*** Update AmeriCorps' policy to require mandatory enforcement of multifactor authentication in the future, including in any hybrid work environment. *(New)*

9. AmeriCorps Must Strengthen Account Management Controls

FY 2021 IG FISMA Metric Area: *Identity and Access Management*

Account management controls help protect against inappropriate access to information systems and unauthorized data modification, loss, and disclosure. For account management controls to be effective, they must be consistently implemented and monitored.

AmeriCorps did not adequately manage user accounts and/or passwords for the network and the Momentum application. For example, AmeriCorps did not disable all network and Momentum accounts of separated employees, did not disable inactive privileged accounts, and did not properly manage passwords that were not changed after a designated timeframe as specified in AmeriCorps' policies.

Specifically, the following issues were noted:

Weaknesses in Account Management for Separated Employees:
Two contractors and three employees, from a total sample of three contractors and six employees who separated between October 1, 2020 and April 12, 2021, maintained access to the network for a range of 11 to 25 days past the individual's date of separation. AmeriCorps' policy requires disabling system accounts within one working day following separation. Management stated a decision was made to not disable system accounts for separated personnel until after their laptops were returned and received by the Helpdesk support team.

In addition, one out of 63 separated employees maintained access to Momentum for four months after separating from AmeriCorps. The employee separated on December 5, 2020 and still maintained access as of April 1, 2021. Management stated that the employee's supervisor mistakenly did not include the employee's Momentum access within the off-boarding request ticket.

Without ensuring accounts are disabled due to separation, AmeriCorps' information is at risk of unauthorized access, increasing the likelihood of unauthorized modification, loss, and disclosure.

Improper Management of Inactive Accounts:
One privileged network account did not log in within 30 days, and one privileged network account never logged on, but the accounts were not disabled in accordance with AmeriCorps' policy, *Cybersecurity Control Families*. Management stated that AmeriCorps did not automatically disable privileged network accounts due to the possibility of a script or processing error. Management indicated they are reviewing a method that utilizes a script to send an email notification of privileged accounts that have not logged in within 30 days to helpdesk personnel in order to determine if accounts require manual disabling.

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 AmeriCorps' information systems.

Weakness in Password Management:
One non-privileged network account did not have a password change within 90 days, as required by AmeriCorps' policy, *Cybersecurity Control Families*, but logged in 175 days after exceeding the 90-day password change requirement. Management stated that they were unable to identify the reason why the user's password exceeded the 90-day maximum lifetime restriction without being reset, and the user was able to log on.

Allowing users to continue to use the same password for an extended period increases the risk that an unauthorized user targeting these accounts will have access longer than if password change deadlines are enforced. Regular password changes limit the period of exposure for a compromised account.

NIST SP 800-53, Revision 4 requires AmeriCorps to create, enable, modify, disable, and remove information system accounts in accordance with AmeriCorps' defined procedures. Furthermore, AmeriCorps 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, (4) are no longer used by applications, services, or the system, and (5) have been inactive for a time-period defined by AmeriCorps. In addition, AmeriCorps is to manage information system authenticators by changing or refreshing authenticators within the organization's defined time-period. The *AmeriCorps Cybersecurity Control Families* document prescribes a one-day period for

deactivating accounts of separated personnel, deactivating inactive accounts after 30 days, and changing passwords every 90 days. AmeriCorps is out of compliance with NIST requirements and with its own policies.

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

The FISMA evaluation for FY 2019[35] recommended that AmeriCorps monitor the employee separation process to ensure AmeriCorps policy is followed for disabling system accounts for separated employees, including removing accounts of separated individuals from the My AmeriCorps Staff Portal Organizational Unit (OU).[36] The FY 2021 evaluation found that no separated individuals maintained access to the My AmeriCorps Staff Portal OU, and we therefore closed this recommendation from FY 2019. However, we continue to find separated individuals who were allowed to maintain access to other AmeriCorps systems, and we are issuing a recommendation related to those systems.

The FISMA evaluation for FY 2019[37] and FY 2020[38] also recommended that AmeriCorps monitor automated scripts to validate that accounts that never logged in and accounts that were inactive for 30 days were disabled in accordance with AmeriCorps policy, and to ensure all AmeriCorps information system passwords are changed at the frequency specified in applicable AmeriCorps policy or the System Security Plan. Our testing found ongoing issues in both of these areas. Accordingly, our prior recommendation remains open, and we are making a new recommendation to address disabling inactive privileged accounts.

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

> ***Recommendation 10:*** Establish an oversight process to ensure that system accounts for separated personnel are disabled within one working day following separated employees' termination, regardless of when the laptop is returned and received. *(New)*
>
> ***Recommendation 11:*** Design and implement a method for identifying inactive privileged accounts via an automated script and manually disabling those accounts, as needed. *(New)*

[35] 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).

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

[37] 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).

[38] Recommendation 8, *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, p. 20, (OIG Report No. 21-03, December 18, 2020).

Security Function: Protect
Maturity Model Scoring

The maturity level based on the 26 IG FISMA Metrics for the "Protect" function is Level 2 (Defined), Not Effective, as depicted in the chart below:

Function	Count	IG FISMA Metrics
Ad Hoc (Level 1)	2	20 and 22
Defined (Level 2)	11	17, 18, 19, 21, 23, 26, 27, 30, 31, 38, and 39
Consistently Implemented (Level 3)	5	24, 28, 32, 35, and 37
Managed and Measurable (Level 4)	6	33, 36, 41*, 43, 44, and 45
Optimized (Level 5)	2	29 and 42
Calculated Maturity Level: Defined (Level 2), Not Effective		

* The maturity scale for Metric 41 stopped at "Managed and Measurable." Therefore AmeriCorps' "Managed and Measurable" maturity level on that particular metric was the highest available rating.

Security Function: Detect
Maturity Model Scoring

The maturity level based on the four IG FISMA Metrics for the "Detect" function is Level 2 (*Defined*) or Not Effective, as depicted in the chart below:

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

The key control weaknesses affecting the "Detect" maturity level including inconsistent vulnerability management, configuration management, and asset management also effect the "Identify" and "Protect" functions and were already addressed in those sections of this report.

10. AmeriCorps Must Test its Incident Response Capability Annually

FY 2021 IG FISMA Metric Area: *Incident Response*

A Federal agency must test its incident response capability in accordance with its established frequency to determine the incident response effectiveness.[39]

AmeriCorps did not test its incident response capability annually as required by AmeriCorps' policy and the *AmeriCorps Incident Response Plan*. The last incident response test was conducted in January 2020. The *AmeriCorps Cybersecurity Control Families* document requires the agency to test its incident response capability at least annually, using checklists, walk-throughs, or tabletop exercises to determine the incident response effectiveness. Additionally, the *AmeriCorps Incident Response Plan* requires convening the Breach Response Team (BRT) annually to hold a tabletop exercise that tests the incident response plan and the BRT's preparedness.

Management stated that an incident response test was not conducted since January 2020 due to resource constraints which resulted in efforts being directed to higher priority tasks. Management also stated that the incident response test will be scheduled after the award of the new Managed IT Services contract.

In the absence of conducting incident response testing and exercises, AmeriCorps is not able to evaluate whether the agency's incident response procedures operate as intended, and personnel may not be appropriately prepared to handle security incidents. Improper incident handling can lead to the loss of confidentiality, integrity and availability of AmeriCorps' data.

To assist AmeriCorps in continuing to strengthen the incident response program, we recommend that AmeriCorps:

> ***Recommendation 12:*** Perform an annual incident response test or exercise in accordance with AmeriCorps' policies. *(New)*

[39] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, control IR-3, Incident Response Testing, page F-104.

Security Function: Respond
Maturity Model Scoring

The maturity level based on the seven IG FISMA Metrics for the function area is Level 3 (*Consistently Implemented*) or Not Effective, as depicted in the chart below:

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

* The maturity scale for Metrics 53 and 57 stopped at "Managed and Measurable." Therefore AmeriCorps' "Managed and Measurable" maturity level on those metrics was the highest available rating.

Security Function: Recover

11. AmeriCorps Must Test its Disaster Recovery Capability and Provide Training Annually

FY 2021 IG FISMA Metric Area: *Contingency Planning*

Federal agencies are required to test their disaster recovery plan and provide disaster recovery training in accordance with the organization defined frequency to determine the effectiveness of the plan and the organizational readiness to execute the plan.[40] The *AmeriCorps Cybersecurity Control Families* document requires conducting contingency plan testing and providing associated training annually. AmeriCorps' *Managed Information Technology Services Disaster Recovery Plan,* Version 1.6, requires annual training and testing of recovery plans, with participants certifying the readiness of their respective systems. At the conclusion of recovery testing, the team memorializes the results, including findings, comments and recommended changes in a memorandum to the Deputy CIO.

AmeriCorps did not conduct the annual disaster recovery test and train disaster recovery personnel for the GSS and the Electronic-System for Programs, Agreements and National Service Participants (eSPAN) systems required by AmeriCorps policy. No disaster recovery test and associated training has occurred since January 2020.

Management stated that the disaster recovery test and associated training was not conducted this year due to responding to changes in the technical environment that required the Managed IT Services (MITS) contractor to build a test replica of the eSPAN system. Management further stated that database administrators have been working to build the new test environment and found gaps in the documentation that prevented the build from being completed. The contractor has been working together with AmeriCorps OIT Infrastructure and Applications team to prioritize resources from both teams in order to complete the build. Management stated that after the build is complete, the disaster recovery test will be completed.

Disaster recovery testing helps to identify recovery weaknesses should a real disaster occur. Therefore, disaster recovery plans that are not tested at least annually place key agency systems at risk of failure in the event of a real disaster or security incident. This may lead to data loss, and decreased staff productivity. A prolonged outage may affect AmeriCorps' ability to perform its mission.

[40] NIST SP 800-53, Revision 4, *Security and Privacy Controls for Federal Information Systems and Organizations*, controls CP-3, Contingency Training and CP-4, Contingency Plan Testing, page F-81.

To assist AmeriCorps in continuing to strengthen the contingency planning program, we recommend that AmeriCorps:

> ***Recommendation 13:*** Establish an oversight process to ensure that the MITS Disaster Recovery Plan is tested for the GSS and eSPAN and associated training is conducted on an annual basis. (New)

Security Function: Recover
Maturity Model Scoring

The maturity level based on the six IG FISMA Metrics for the function area is Level 3 (*Consistently Implemented*) or Not Effective, as depicted in the chart below.

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

* The maturity scale for Metrics 64 stopped at "Managed and Measurable." Therefore AmeriCorps' "Managed and Measurable" maturity score on that metrics was the highest available rating.

Appendix I

BACKGROUND

AmeriCorps[41] 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. AmeriCorps has a FISMA inventory of eight information systems – the Network or GSS, eSPAN (which includes the eGrants grants management system), Momentum, AmeriCorps Health Benefits, AmeriCorps Childcare Benefits System, Presidential Volunteer Service Awards, Online Ordering system, and public websites. The first six of these systems are categorized as moderate security, while the Online Ordering system and public websites are rated as low security.[42] All eight systems are hosted and operated by third-party service providers, although AmeriCorps hosts certain components of the GSS. AmeriCorps' network consists of multiple sites: HQ, one Field Financial Management Center, and four NCCC campuses. These facilities are connected through commercially managed telecommunications network connections.

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

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

AmeriCorps establishes specific organization-defined IT security policies, procedures, and parameters in its *Cybersecurity Control Families* document, which incorporates the NIST SP 800-53, Revision 4.

[41] Effective on October 15, 2020, the operating name of the agency was changed from Corporation for National and Community Service to AmeriCorps.

[42] 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 to establish Agency baseline security requirements.

FY 2021 IG FISMA Reporting Metrics

OMB and DHS annually provide instructions to Federal agencies and IGs for preparing FISMA reports. On November 9, 2020, OMB issued Memorandum M-20-04, *Fiscal Year 2020-2021 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 2021 Inspector General Federal Information Security Modernization Act of 2014 Reporting Metrics* (IG FISMA Metrics), provided reporting requirements across key areas to be addressed in the independent assessment of agencies' information security programs.[43]

[43] https://www.cisa.gov/publication/fy21-fisma-documents

Appendix I

The FY 2021 IG FISMA Metrics incorporate a maturity model that aligns with the five functional areas in the NIST *Framework for Improving Critical Infrastructure Cybersecurity* (Cybersecurity Framework), version 1.1 Identify, Protect, Detect, Respond and Recover. The Cybersecurity Framework provides agencies with a common structure for identifying and managing cybersecurity risks across the enterprise IT and provides IGs with a method for assessing the maturity of controls to address those risks, as highlighted in **Table 2**.

Table 2: Aligning the NIST Cybersecurity Framework Security Functions to the FY 2021 IG FISMA Metric Domains

NIST Cybersecurity Framework Security Functions	FY 2021 IG FISMA Metrics Domains
Identify	Risk Management and Supply Chain Risk Management[44]
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 3** 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 3: 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.

[44] Ibid 5.

Appendix II

OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

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

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.[45] The evaluation was designed to assess the effectiveness of AmeriCorps' 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 AmeriCorps' 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 AmeriCorps implemented for safeguarding PII and reporting incidents involving PII, protecting sensitive 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 20, 2021 to October 8, 2021. A network vulnerability assessment was also conducted at HQ.

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

In addition, the evaluation included an assessment of effectiveness for each of the nine[46] FY 2021 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 AmeriCorps made progress in implementing the recommended improvements concerning its information security program.[47]

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 2021 IG FISMA Metrics Domains aligned with the Cybersecurity Framework Security Functions.[48] **Table 4** lists the selected controls for the four AmeriCorps systems that were reviewed for this evaluation:

Table 4: List of Selected Controls Reviewed

Security Control Family	NIST 800-53 Associated Control[49]
Access Control	AC-1, AC-2, AC-17, and AC-19
Awareness and Training	AT-1, AT-2, and AT-3
Security Assessment and Authorization	CA-1, CA-2, CA-3, CA-5, CA-6, and CA-7
Configuration Management	CM-1, CM-2, CM-3, CM-6, CM-7, CM-8, and CM-9
Contingency Planning	CP-1, CP-2, CP-3, CP-4, CP-6, CP-7, CP-8, and CP-9
Identification and Authentication	IA-1 and IA-2
Incident Response	IR-4, IR-6, IR-7, and IR-8
Media Protection	MP-3 and MP-6
Planning	PL-2, PL-4, and PL-8
Program Management	PM-5, PM-11, and PM-30
Personnel Security	PS-1, PS-2, and PS-6
Risk Assessment	RA-2, RA-3, and RA-5
Supply Chain Risk Management	SR-1, SR-3, SR-5, SR-6, and SR-11
System and Services Acquisition	SA-3, SA-8, and SA-12
System and Information Integrity	SI-2, SI-3, SI-4, and SI-7
System and Communications Protection	SC-8 and SC-28
Privacy	AR-1, AR-2, AR-4, AR-5, and SE-2

[46] Ibid 5.

[47] *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, (OIG Report No. 21-03, December 18, 2020).

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

[49] These associated controls are from NIST SP 800-53, Revision 4. This document has been superseded by NIST SP 800-53, Revision 5, and remains in effect until September 23, 2021.

To accomplish the evaluation objective, we:

- Interviewed key personnel and reviewed legal and regulatory requirements stipulated by FISMA.
- Reviewed documentation related to AmeriCorps' information security program, such as security policies and procedures, system security plans, security control assessments, risk assessments, security assessment authorizations, plan of action and milestones, incident response plan, configuration management plan, and continuous monitoring plan.
- Tested system processes to determine the adequacy and effectiveness of selected controls.
- Reviewed the status of recommendations in the FY 2020 FISMA report, including supporting documentation, to ascertain whether the actions taken addressed the weakness.[50] See Appendix III for the status of prior years' recommendations.

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

- Memorandum M-20-04, *Fiscal Year 2020-2021 Guidance on Federal Information Security and Privacy Management Requirements*.
- FY 2021 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).

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

[50] *Fiscal Year 2020 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, (OIG Report No. 21-03, December 18, 2020).

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 2017, 2018, 2019, and 2020 FISMA evaluations.[51] [52] [53] [54]

During FY 2021, AmeriCorps implemented corrective actions to close eight prior years' recommendations from the FY 2017 - 2020 FISMA evaluations. An additional 3 open recommendations were closed because they were superseded by FY 2019 recommendations that remain open, and new FY 2021 recommendations.

Status of Prior Year FY Recommendations

FY 2017 FISMA Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations
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.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the policy was implemented.
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	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the controls were implemented.

[51] 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).
[52] 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).
[53] *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).
[54] Ibid 50.

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	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the controls were implemented.
FY 2018 FISMA Evaluation	**Status Determined by AmeriCorps**	**Auditor Position on Status of Recommendations**
Recommendation 2: Ensure that OIT evaluates if the internet connections at the Field Financial Management Center, National Civilian Community Corps Campuses, and State Office is sufficient to allow patches to be deployed to all devices within the defined risk-based patch timeline in CNCS policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections.	Closed	Closed This recommendation is superseded by FY 2019 recommendation 2.
FY 2019 FISMA Evaluation	**Status Determined by AmeriCorps**	**Auditor Position on Status of Recommendations**
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 AmeriCorps 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 5

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 AmeriCorps policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections.	Closed	Remains Open AmeriCorps did not provide evidence to validate that OIT evaluated if the internet connections at the National Civilian Community Corps Campuses and Regional Offices were sufficient for timely patching of all devices.
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.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the process was implemented.
Recommendation 5: Develop and implement a written process to ensure Remedyforce tickets are completed at the time the inventory is updated.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the process was implemented.
Recommendation 6: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the process was implemented.
Recommendation 7: Perform and document analysis to determine the feasibility of completely automating the inventory management process.	Open	Remains Open Refer to Finding 2
Recommendation 8: Continue the current effort to complete a comprehensive risk register at the mission and business process level.	Closed	Remains Open AmeriCorps did not complete the mission/business process level risk register.
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	Closed	Remains Open Refer to Finding 1

steady, measurable improvement towards an effective information security program.		
Recommendation 10: Establish and document standard baseline configurations for all platforms in the AmeriCorps information technology environment and ensure these standard baseline configurations are appropriately implemented, tested, and monitored for compliance with established AmeriCorps security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Open	Remains Open Modified Repeat, refer to Finding 6
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 8
Recommendation 12: Complete the implementation of Personal Identification Verification multifactor authentication for network access for all non-privileged users by upgrading all users to Microsoft Windows 10 workstations and enforcing logon with a Personal Identification Verification card.	Open	Remains Open Although Microsoft Windows 10 workstations are no longer in use, AmeriCorps did not enforce PIV for system users. Refer to Finding 8
Recommendation 13: Develop and implement a written process for the Director of Infrastructure to monitor the employee separation process to ensure AmeriCorps 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	Closed This recommendation is superseded by FY 2021 recommendation 9.
Recommendation 14: Enhance information systems to automatically disable user accounts after 30 days of inactivity in accordance with AmeriCorps policy. This includes monitoring automated scripts to validate accounts are disabled properly.	Closed	Remains Open Refer to Finding 9
Recommendation 16: Develop and Implement a written process that ensures all AmeriCorps information system passwords are changed at the frequency specified in applicable AmeriCorps policy or the System Security Plan.	Closed	Remains Open Refer to Finding 9

Recommendation 18: Complete background investigations in accordance with the developed schedule based on prioritization of higher-level risk.	Closed	Closed
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.	Closed	Closed
Recommendation 20: Develop and implement a written process to ensure the Office of Human Capital completes background investigations for all contractors.	Closed	Closed
Recommendation 21: Assess the NCCC campus member credentialing process and mechanism to ensure compliance with AmeriCorps personnel security policy for badging.	Closed	Closed
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.	Closed	Closed
Recommendation 23: Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the recommendation was implemented.
Recommendation 24: Periodically provide training for the NCCC campus personnel on the data retention and disposal requirements.	Closed	Closed
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.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the recommendation was implemented.
Recommendation 28: Secure the networking infrastructure located at the NCCC Southwest Region Campus in a locked room or cage.	Closed	Closed

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 Finding 1
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
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 Finding 1
FY 2020 FISMA Evaluation	**Status Determined by AmeriCorps**	**Auditor Position on Status of Recommendations**
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.	Closed	Closed This recommendation is superseded by FY 2021 recommendation 2.
Recommendation 2: Specify how quickly users must apply security and operating system updates on AmeriCorps mobile devices, and implement a process to deny access to AmeriCorps enterprise services for mobile devices that have not been updated within the prescribed period.	Open	Remains Open
Recommendation 3: Develop and implement a process to block unauthorized applications from installing on AmeriCorps mobile devices.	Open	Remains Open
Recommendation 4: Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations.	Open	Remains Open
Recommendation 5: Fully implement standard baseline configurations for all platforms in the AmeriCorps information technology environment and establish processes to test and monitor for	Open	Remains Open

compliance with established AmeriCorps security standards.		
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.	Closed	Remains Open Refer to Finding 8
Recommendation 7: Ensure AmeriCorps system administrators validate user accounts are approved prior to granting Momentum access.	Closed	Closed
Recommendation 8: Ensure that accounts for users that never logged in are included in the AmeriCorps Inactive script.	Closed	Remains Open Refer to Finding 9
Recommendation 9: Ensure all personnel whose responsibilities include access to PII complete annual privacy-role based training.	Open	Remains Open

Appendix IV

MANAGEMENT COMMENTS

To: Monique P. Colter, Assistant Inspector General for Audit

From: Pape Cisse, Chief Information Officer (CIO)

Cc: Malcom Coles, Acting Chief Executive Officer
Jenny Mauk, Chief of Staff
Gina Cross, Acting Chief Operating Officer
Bilal Razzaq, Chief Information Security Officer
Fernando Laguarda, General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits and Investigations Program Manager
Sarah Mirzakhani, Principal, CliftonLarsonAllen LLP

Date: November 15, 2021

Subject: Response to Request for Comments on the Office of Inspector General Draft Report on the Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of AmeriCorps

This is the formal response to the Office of Inspector General's Draft Report: Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of AmeriCorps.

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

1. AmeriCorps Must Develop and Implement a Strategy, Including Enforcing Accountability within the Office of Information Technology, for Improving its Information Security Program to an Effective Level

Recommendation 1: Design and implement an effective accountability system that includes clear expectations of goals, performance measures, estimated target dates, and monitoring to hold OIT leadership accountable for improving AmeriCorps' information security program to an effective level. (New)

AmeriCorps Response: Concur. AmeriCorps' Leadership is dedicated to addressing the issues identified by the OIG. AmeriCorps will ensure all parties are held accountable for improving the information security program.

2. AmeriCorps Must Improve Its Inventory Management Process

Recommendation 2: Complete asset tracking refresher training for the Tier 2 support team. (New)

AmeriCorps.gov
250 E Street SW
Washington, D.C. 20525
202-606-5000/ 800-942-2677

AmeriCorps Response: Concur. OIT is in the process of competition of its IT Services contract. Part of the onboarding process of the new contract is to train all Tier 2 support team personnel.

Recommendation 3: Update the AmeriCorps SOP Asset Tracking Procedures to include a process for the Tier 2 Lead to review the IT asset inventory to ensure the required fields for the information technology assets are documented; and implement the new process. (New)

AmeriCorps Response: Concur. AmeriCorps will update and enhance the existing Asset Tracking Procedures to include a process for the Tier 2 Lead to review the inventory implementing quality control to ensure timeliness and quality of the asset tracking.

3. AmeriCorps Must Maintain Current Interconnection Security Agreements (ISA)

Recommendation 4: Complete and execute the ISA with the Social Security Administration. (New)

AmeriCorps Response: Concur. AmeriCorps updated the ISA with Social Security Administration. The document has been updated and signed by all parties on October 22, 2021. The signed ISA will be submitted to the OIG for closure of this finding.

Recommendation 5: Document and implement an annual review process to validate that all agreements for system interconnections are kept current. (New)

AmeriCorps Response: Concur. AmeriCorps will ensure the System Owners and System Security Officers review agreements with outside agencies annually and ensure all agreement are completed before they expire.

4. AmeriCorps Must Develop a Supply Chain Risk Management Strategy and Related Policies and Procedures

Recommendation 6: Develop, document, and communicate an overall SCRM strategy, implementation plan, and related policies and procedures to guide and govern supply chain risk management activities. If AmeriCorps intends to limit its IT purchases to GSA vendors, it should so state, and indicate who, if anyone, must approve exceptions. (New)

AmeriCorps Response: Concur. As a smaller agency, AmeriCorps buys all products through the GSA Schedule which does ensure proper supply chain management. AmeriCorps will be augmenting its purchasing policies to ensure these requirements are clearly stated and understood and document how exceptions will be reviewed and approved.

5. AmeriCorps 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.

Recommendation: The FY 2019 recommendations remain open, and CLA is not making additional recommendations at this time.

AmeriCorps Response: Concur. The remediation is ongoing, and AmeriCorps is on track to complete this remediation by September 2023. As OIT procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with OIT policies and procedures.

6. AmeriCorps Must Implement Standard Baseline Configurations

The FY 2019 and FY 2020 FISMA evaluation reports made recommendations for AmeriCorps to establish and document standard baseline configurations for all platforms in the AmeriCorps IT environment and to ensure that these standard baseline configurations were appropriately implemented, tested, and monitored for compliance with established AmeriCorps security standards.

Recommendation: The FY 2019 and 2020 recommendations remain open, and we are not making additional recommendations related to baseline configuration controls.

AmeriCorps Response: Concur. OIT Management is working to develop and monitor baseline configurations in accordance with FISMA requirements, NIST guidelines and AmeriCorps security standards.

7. AmeriCorps Must Properly Document the Security Impact Analysis (SIA) for Information System Changes

Recommendation 7: Update the SIA SOP to require maintaining completed SIA questionnaires in the change management tool for all system changes for validating whether each configuration change requires a SIA. (New)

AmeriCorps Response: Concur. AmeriCorps will update the SIA SOP and utilize existing technologies to automate the process with SharePoint Workflow to ensure each System Owner prepares and tracks the SIA questionnaire in accordance with AmeriCorps policy.

8. AmeriCorps Must Enforce Multifactor Authentication for Information System 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.

Recommendation 8: Immediately reinstate mandatory enforcement of multifactor authentication in accordance with CISA's recommendation. (New)

AmeriCorps Response: Concur. AmeriCorps will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. AmeriCorps is working with staff to ensure each user has a PIV card. Once completed PIV authentication will be enforced for all users. The target date for full implementation is the end of March 2022.

Recommendation 9: Update AmeriCorps' policy to require mandatory enforcement of multifactor authentication in the future, including in any hybrid work environment. (New)

AmeriCorps Response: Concur. OIT will ensure the Cybersecurity and Account Management policies are updated to accurately reflect the requirement for enforced PIV authentication.

9. AmeriCorps Must Strengthen Account Management Controls

Recommendation 10: Establish an oversight process to ensure that system accounts for separated personnel are disabled within one working day following separated employees' termination, regardless of when the laptop is returned and received. (New)

AmeriCorps Response: Concur. OIT will work with Human Capital to enhance the existing process for monthly assessments of account management procedures and implement quality controls to ensure account information is updated within one working day of personnel actions.

Recommendation 11: Design and implement a method for identifying inactive privileged accounts via an automated script and manually disabling those accounts, as needed. (New)

AmeriCorps Response: Concur. AmeriCorps will update the current script to identify inactive accounts and implement a manual process for reviewing the results and disabling privileged accounts as needed.

10. AmeriCorps Must Test its Incident Response Capability Annually

Recommendation12: Perform an annual incident response test or exercise in accordance with AmeriCorps' policies. (New)

AmeriCorps Response: Concur. As part of the new information technology (IT) service contract, Incident Response (IR) Testing will be conducted annually to ensure the IR Team is ready to respond when needed.

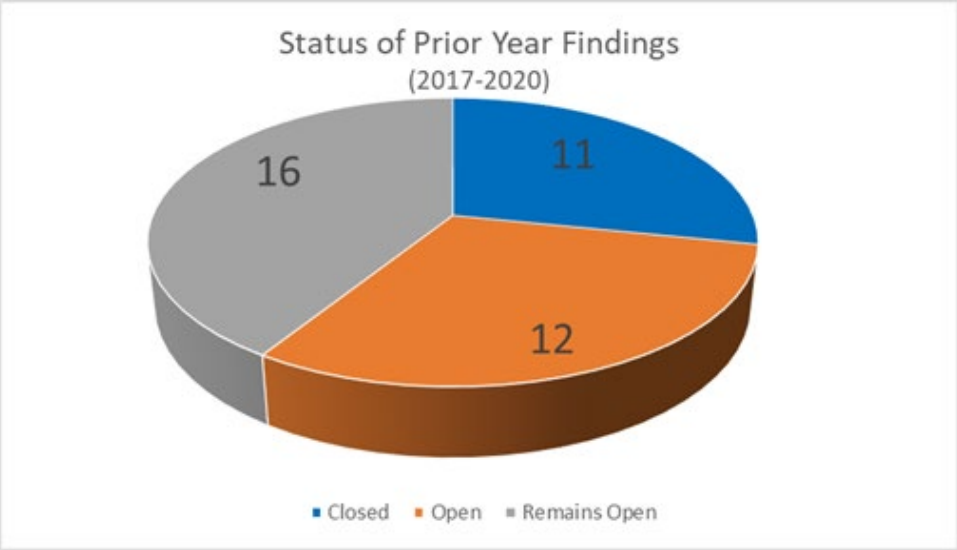
11. AmeriCorps Must Test its Disaster Recovery Capability and Provide Training Annually

Recommendation13: Establish an oversight process to ensure that the MITS Disaster Recovery Plan is tested for the GSS and eSPAN and associated training is conducted on an annual basis. (New)

AmeriCorps Response: Non-concur. AmeriCorps agrees that Disaster Recovery testing has not been completed yet this year, but as previously stated, some systems, like the GSS, choose to combine IR and DR testing. This recommendation is duplicative with Recommendation 12 and will be satisfied when the testing from Recommendation 12 is completed.

Status of Prior Year Findings

Out of the 39 findings from 2017-2020, the auditors have agreed to close eleven of those. An additional sixteen findings have been closed by AmeriCorps but remain open after the auditors determined there was insufficient evidence to close them. AmeriCorps is in the process of reviewing those sixteen items to determine what additional remediations need to be addressed. The remaining twelve items, AmeriCorps acknowledges are open and are on schedule to be remediated.



FY	Evaluation	Status Determined by AmeriCorps	Auditor Position on Status of Recommendations	AmeriCorps Response
FY 17	**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.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the policy was implemented.	Updating mobile device policy and procedures to enhance security restrictions.

FY 17	**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	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the controls were implemented.	This has been completed and requires a site visit from the auditors to validate.
FY 17	**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	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the controls were implemented.	This has been completed and requires a site visit from the auditors to validate.
FY 18	**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	Closed	Closed This recommendation is superseded by FY 2019 recommendation 2.	This has been completed and requires a site visit from the auditors to validate.

	policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections.			
FY 19	**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 AmeriCorps 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 5	AmeriCorps concurs. As OIT procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with OIT policies and procedures.

FY 19	**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 AmeriCorps policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections.	Closed	Remains Open AmeriCorps did not provide evidence to validate that OIT evaluated if the internet connections at the National Civilian Community Corps Campuses and Regional Offices were sufficient for timely patching of all devices.	This has been completed and requires a site visit from the auditors to validate.
FY 19	**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.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the process was implemented.	AmeriCorps will update and enhance the existing Asset Tracking Procedures to include a process to review the inventory is properly maintained.
FY 19	**Recommendation 5**: Develop and implement a written process to ensure Remedyforce tickets are completed at the time the inventory is updated.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the process was implemented.	AmeriCorps will update and enhance the existing Asset Tracking Procedures to include a process to review the inventory is properly maintained.
FY 19	**Recommendation 6**: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the	AmeriCorps will update and enhance the existing Asset Tracking

Appendix IV

			process was implemented.	Procedures to include a process to review the inventory is properly maintained.
FY 19	**Recommendation 7**: Perform and document analysis to determine the feasibility of completely automating the inventory management process.	Open	Remains Open Refer to Finding 2	OIT is in the process of procuring an IT Services contract. Part of the onboarding process of the new contract is to train all Tier 2 support team. AmeriCorps will update and enhance the existing Asset Tracking Procedures to include a process to review the inventory to ensure required fields are documented.
FY 19	**Recommendation 8:** Continue the current effort to complete a comprehensive risk register at the mission and business process level.	Closed	Remains Open AmeriCorps did not complete the mission/business process level risk register.	OCRO is working to update existing processes to develop comprehensive risk register.

FY 19	**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 Finding 1	AmeriCorps' Leadership is dedicated to addressing the issues identified by the OIG. AmeriCorps will ensure all parties are held accountable for improving the information security program.
FY 19	**Recommendation 10:** Establish and document standard baseline configurations for all platforms in the AmeriCorps information technology environment and ensure these standard baseline configurations are appropriately implemented, tested, and monitored for compliance with established AmeriCorps security standards. This includes documenting approved deviations from the configuration baselines with business justifications.	Open	Remains Open Modified Repeat, refer to Finding 6	As OIT procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with OIT policies and procedures.
FY 19	**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 8	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing

				downtime to the user base. Management will ensure policies are updated to accurately reflect the requirement for enforced PIV authentication.
FY 19	**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 Although Microsoft Windows 10 workstations are no longer in use, AmeriCorps did not enforce PIV for system users. Refer to Finding 8	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. Management will ensure policies are updated to accurately reflect the requirement for enforced PIV authentication.
FY 19	**Recommendation 13:** Develop and implement a written process for the Director of Infrastructure to monitor the employee separation process to ensure AmeriCorps policy is followed for disabling system accounts within one working day following separated employees' termination and disabled network accounts of separated individuals are	Open	Closed This recommendation is superseded by FY 2021 recommendation 9.	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. Management

	removed from the Active Directory My AmeriCorps Staff Portal Organizational Unit.			will ensure policies are updated to accurately reflect the requirement for enforced PIV authentication.
FY 19	**Recommendation 14:** Enhance information systems to automatically disable user accounts after 30 days of inactivity in accordance with AmeriCorps policy. This includes monitoring automated scripts to validate accounts are disabled properly.	Closed	Remains Open Refer to Finding 9	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. Management will ensure policies are updated to accurately reflect the requirement for enforced PIV authentication.
FY 19	**Recommendation 16:** Develop and Implement a written process that ensures all AmeriCorps information system passwords are changed at the frequency specified in applicable AmeriCorps policy or the System Security Plan.	Closed	Remains Open Refer to Finding 9	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. Management will ensure policies are updated to

				accurately reflect the requirement for enforced PIV authentication.
FY 19	**Recommendation 18:** Complete background investigations in accordance with the developed schedule based on prioritization of higher-level risk.	Closed	Closed	
FY 19	**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.	Closed	Closed	
FY 19	**Recommendation 20**: Develop and implement a written process to ensure the Office of Human Capital completes background investigations for all contractors.	Closed	Closed	
FY 19	**Recommendation 21:** Assess the NCCC campus member credentialing process and mechanism to ensure compliance with AmeriCorps personnel security policy for badging.	Closed	Closed	

Appendix IV

FY 19	**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.	Closed	Closed	
FY 19	**Recommendation 23:** Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the recommendation was implemented.	This has been completed and requires a site visit from the auditors to validate.
FY 19	**Recommendation 24:** Periodically provide training for the NCCC campus personnel on the data retention and disposal requirements.	Closed	Closed	
FY 19	**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.	Closed	Remains Open AmeriCorps did not provide sufficient evidence to validate the recommendation was implemented.	This has been completed and requires a site visit from the auditors to validate.
FY 19	**Recommendation 28:** Secure the networking infrastructure located at the NCCC Southwest Region Campus in a locked room or cage.	Closed	Closed	
FY 19	**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	Closed	Remains Open Refer to Finding 1	AmeriCorps' Leadership is dedicated to addressing the issues identified by the OIG. AmeriCorps will ensure all parties are held

	steady, measurable improvement towards becoming an effective information security program.			accountable for improving the information security program.
FY 19	**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	Satellite offices 60% integrated into HQ administration and security practices.
FY 19	**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 Finding 1	AmeriCorps' Leadership is dedicated to addressing the issues identified by the OIG. AmeriCorps will ensure all parties are held accountable for improving the information security program.
FY 20	**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.	Closed	Closed This recommendation is superseded by FY 2021 recommendation 2.	AmeriCorps will update and enhance the existing Asset Tracking Procedures to include a process to review the inventory to ensure required fields are documented.

FY 20	**Recommendation 2:** Specify how quickly users must apply security and operating system updates on AmeriCorps mobile devices, and implement a process to deny access to AmeriCorps enterprise services for mobile devices that have not been updated within the prescribed period.	Open	Remains Open	Updating mobile device policy and procedures to specify the timeframe for implementing mobile patches.
FY 20	**Recommendation 3:** Develop and implement a process to block unauthorized applications from installing on AmeriCorps mobile devices.	Open	Remains Open	Updating mobile device policy and procedures to specify the timeframe for implementing mobile patches.
FY 20	**Recommendation 4:** Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations.	Open	Remains Open	As OIT procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with OIT policies and procedures.

Appendix IV

FY 20	**Recommendation 5:** Fully implement standard baseline configurations for all platforms in the AmeriCorps information technology environment and establish processes to test and monitor for compliance with established AmeriCorps security standards.	Open	Remains Open	As OIT procures a new information technology (IT) service contract, there will be specific service level agreements (SLA) in place that directly address the service provider's responsibility to maintain a secure network in accordance with OIT policies and procedures.
FY 20	**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.	Closed	Remains Open Refer to Finding 8	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. Management will ensure policies are updated to accurately reflect the requirement for enforced PIV authentication.
FY 20	**Recommendation 7:** Ensure AmeriCorps system administrators validate user	Closed	Closed	

	accounts are approved prior to granting Momentum access.			
FY 20	**Recommendation 8:** Ensure that accounts for users that never logged in are included in the AmeriCorps Inactive script.	Closed	Remains Open Refer to Finding 9	Management will assess the impact of enforcing PIV access and implement as quickly as possible, minimizing downtime to the user base. Management will ensure policies are updated to accurately reflect the requirement for enforced PIV authentication.
FY 20	**Recommendation 9:** Ensure all personnel whose responsibilities include access to PII complete annual privacy-role based training.	Open	Remains Open	Awaiting replacement for AmeriCorps Privacy lead.

OFFICE OF INSPECTOR GENERAL

AmeriCorps

250 E St., SW, Suite 4100
Washington, DC 20525

OFFICE OF INSPECTOR GENERAL
HOTLINE: 1.800.452.8210
HOTLINE@AmeriCorpsOIG.gov | AmeriCorpsOIG.gov