AmeriCorps
Office of Inspector General

FY 2024 Federal Information Security Modernization Act (FISMA) Audit

Audit Report

Number: OIG-AR-24-03

November 14, 2024

AmeriCorps
Office of Inspector General

November 14, 2024

MEMORANDUM TO: Prabhjot Bajwa
Chief Information Officer

FROM: Lauren Lesko
LAUREN LESKO
Digitally signed by LAUREN LESKO
Date: 2024.11.14 16:40:51 -05'00'
Acting Assistant Inspector General for Audits

SUBJECT: Fiscal Year 2024 Federal Information Security Modernization Act Audit (OIG Report- AR-24-03)

Enclosed is the AmeriCorps Office of Inspector General (OIG) final report on the Fiscal Year (FY) 2024 Federal Information Security Modernization Act (FISMA) Audit, OIG Report AR-24-03.

AmeriCorps OIG contracted with the independent certified public accounting firm of RMA Associates, LLC (RMA) to conduct the FY 2024 FISMA audit. RMA is responsible for the attached final report. We reviewed RMA'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 RMA did not comply with the *Generally Accepted Government Auditing Standards,* issued by the Comptroller General of the United States.

If you have any questions or wish to discuss the report, please contact me at (202) 880-9292 or l.lesko@americorpsoig.gov.

cc: Michael D. Smith, 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
Andrea Grill, Acting General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits and Investigations Program Manager
Stephen Ravas, Acting Inspector General
Pamela Van Dort, Acting Deputy Inspector General
Meliha Tokay, Special Assistant to the Chief of Staff and Assistant to the Board of Directors
Marc Hebert, Partner, RMA Associates, LLC

RMA Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

AMERICORPS

FEDERAL INFORMATION SECURITY MODERNIZATION ACT AUDIT REPORT

FISCAL YEAR 2024

NOVEMBER 14, 2024

FINAL REPORT

RMA Associates
Auditors. Consultants. Advisors.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

REPORT NOTICE—NDAA REQUIREMENT

THIS REPORT IS INTENDED SOLELY FOR THE INFORMATION AND USE OF THE AMERICORPS OIG, AMERICORPS, AND U.S. CONGRESS AND IS NOT INTENDED TO BE, AND SHOULD NOT BE, USED BY ANYONE OTHER THAN THESE SPECIFIED PARTIES. PURSUANT TO P.L. 117-263, SECTION 5274, NON-GOVERNMENTAL ORGANIZATIONS AND BUSINESS ENTITIES IDENTIFIED IN THIS REPORT HAVE THE OPPORTUNITY TO SUBMIT A WRITTEN RESPONSE FOR THE PURPOSE OF CLARIFYING OR PROVIDING ADDITIONAL CONTEXT TO ANY SPECIFIC REFERENCE. COMMENTS MUST BE SUBMITTED WITHIN 30 DAYS OF THE REPORT ISSUANCE DATE.

FURTHER, PURSUANT TO P.L. 117-263, SECTION 5274, NON-GOVERNMENTAL ORGANIZATIONS AND BUSINESS ENTITIES IDENTIFIED IN THIS REPORT HAVE THE OPPORTUNITY TO SUBMIT A WRITTEN RESPONSE FOR THE PURPOSE OF CLARIFYING OR PROVIDING ADDITIONAL CONTEXT TO ANY SPECIFIC REFERENCE. COMMENTS MUST BE SUBMITTED TO L.LESKO@AMERICORPSOIG.GOV WITHIN 30 DAYS OF THE REPORT ISSUANCE DATE AND WE REQUEST THAT COMMENTS NOT EXCEED 2 PAGES. THE COMMENTS WILL BE APPENDED BY LINK TO THIS REPORT AND POSTED ON OUR PUBLIC WEBSITE. WE REQUEST THAT SUBMISSIONS BE SECTION 508 COMPLIANT AND FREE FROM ANY PROPRIETARY OR OTHERWISE SENSITIVE INFORMATION.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Table of Contents

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Executive Summary

Introduction

The Federal Information Security Modernization Act of 2014 (FISMA)[1] requires Federal agencies to conduct an annual independent audit of their information security program and practices to be performed by the Inspector General or an independent external auditor. AmeriCorps' Office of Inspector General (OIG) contracted with the independent certified public accounting firm of RMA Associates, LLC (RMA) to conduct the FISMA audit for Fiscal Year (FY) 2024.

The objective of this audit was to determine the effectiveness of AmeriCorps' information security program and practices for the period August 1, 2023, through July 31, 2024, and report the results to the Office of Management and Budget (OMB). This report presents the results of RMA's independent audit of AmeriCorps' information security program and practices in accordance with FISMA. The audit included the testing of select management, technical, and operational controls outlined in the National Institute of Standards and Technology (NIST) guidance for four internal and external AmeriCorps' information systems:

- General Support System (GSS);
- Electronic-System for Programs, Agreements and National Service Participants (eSPAN);
- Administrative Resource Center (ARC) Financial System; and
- A financial management system.

AmeriCorps relies on its information technology (IT) systems to make grants and manage a residential national service program. AmeriCorps' information security program must protect these systems from malicious attacks and other compromises that may put its sensitive information, including personally identifiable information (PII), at risk.

A functional information security area is not considered effective unless it achieves a rating of at least *Managed and Measurable* (Level 4).

Table 1 explains the five maturity model levels. The lower (foundational) levels of the maturity model focus on developing sound, risk-based policies, and procedures, while the advanced levels leverage automation and near real-time monitoring to achieve the institutionalization and effectiveness of those policies and procedures.

[1] Public Law (P.L.) 113-283, Federal Information Security Modernization Act of 2014, December 18, 2014.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Table 1: IG Audit Maturity Levels

Maturity Level	Maturity Level Description
Ad Hoc (Level 1)	Policies, procedures, and strategy are not formalized; activities are performed in an ad-hoc, reactive manner.
Defined (Level 2)	Policies, procedures, and strategy are formalized and documented but not consistently implemented.
Consistently Implemented (Level 3)	Policies, procedures, and strategy are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Managed and Measurable (Level 4)	Quantitative and qualitative measures of the effectiveness of policies, procedures, and strategy are collected across the organization and used to assess them and make necessary changes.
Optimized (Level 5)	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.

Audit Results

We determined AmeriCorps' information security program improved overall but is still considered not effective because the information security program was not consistent with applicable FISMA requirements, OMB policy and guidance, or NIST standards and guidelines for the period of August 1, 2023, through July 31, 2024. We determined AmeriCorps' control processes were operational and generated information that supported control monitoring and decision-making. Improvements were made by the agency on two functions, Detect and Recover, each receiving an FY 2024 maturity level of *Consistently Implemented* (Level 3). Additionally, we identified seven weaknesses across the nine FISMA domains indicating areas of improvement for AmeriCorps. The identified conditions were evaluated from a risk-based standpoint and within the context of the overall information security program to determine their root cause and associated level of risk. AmeriCorps should implement further internal controls as identified in this report, including implementing the ten open prior year recommendations to facilitate reaching the benchmark for an effective information security program, *Managed and Measurable* (Level 4).

The Office of the Chief Information Officer is required to monitor and evaluate the performance of the information security program and practices based on performance measurements. AmeriCorps has maintained or improved its maturity and effectiveness levels relative to FY2023, as presented in **Table 2**.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Table 2: FY 2023 – FY 2024 Maturity Level Comparison

Function	FY 2023 Maturity	FY 2024 Maturity
Identify	Consistently Implemented	Consistently Implemented
Protect	Consistently Implemented	Consistently Implemented
Detect	Defined	Consistently Implemented
Respond	Consistently Implemented	Consistently Implemented
Recover	Defined	Consistently Implemented
Overall Maturity:	**Consistently Implemented**	**Consistently Implemented**
Overall Effectiveness:	**Not Effective**	**Not Effective**

AmeriCorps made considerable progress in implementing prior year recommendations. During FY 2024, AmeriCorps resolved 19 of 29 open recommendations from prior years, thus improving the IG FISMA Metrics results. However, further improvements in information security are still needed for the program to be rated effective. We identified three new recommendations in addition to the ten prior year recommendations that remain open. See **Appendix III** for the status of prior year recommendations.

The control weaknesses that prevent AmeriCorps from maturing its information security program relate to the following metrics:

1. Inventory Management;
2. Supply Chain Risk Management Program;
3. Vulnerability and Patch Management Program;
4. Personnel Screening Process;
5. Authorization Packages;
6. Logging; and
7. Contingency Planning.

These control weaknesses affected the maturity levels of the functional areas of information security as shown in **Table 3**.

Table 3: FY 2024 Function Area Control Weaknesses

Function	Domain	Control Weakness	FY 2024 Assessed Maturity
Identify	Risk Management Supply Chain Risk Management (SCRM)	AmeriCorps did not enforce the requirement for the Tier 2 lead to perform the monthly audit of the inventory report. (*Finding 1*) AmeriCorps did not develop, document, and communicate SCRM procedures to address all FISMA SCRM requirements. (*Finding 2*)	Consistently Implemented

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Function	Domain	Control Weakness	FY 2024 Assessed Maturity
Protect	Configuration Management Identity and Access Management Data Protection and Privacy Security Training	AmeriCorps did not implement a process to track the patching of network devices and servers by the defined risk-based patch timelines in AmeriCorps' policy. Also, AmeriCorps did not ensure replacement of information system components when support for the components was no longer available. Additionally, AmeriCorps did not monitor and record actions taken by the contractor to ensure vulnerability remediation for network devices and servers was addressed or the exposure to unpatchable vulnerabilities was minimized. Finally, AmeriCorps did not enhance the inventory process to ensure all devices were properly identified and monitored. (*Finding 3*) AmeriCorps did not develop and implement a written oversight process to ensure that Contracting Officer's Representatives regularly provide the Office of Human Capital with names of contractors who require background investigations and that the Office of Information Technology (OIT) confirms those background investigations are complete before contractors receive system access. (*Finding 4*)	Consistently Implemented
Detect	Information Security Continuous Monitoring	AmeriCorps did not complete the Authorization To Use (ATU) package that covers the ARC Financial System. (*Finding 5*)	Consistently Implemented
Respond	Incident Response	AmeriCorps did not upgrade and configure its Security Information and Event Management (SIEM) tool to capture all log requirements in accordance with OMB M-21-31. In addition, AmeriCorps did not perform a gap analysis by reconciling all SIEM solutions that are capturing logs. (*Finding 6*)	Consistently Implemented

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Function	Domain	Control Weakness	FY 2024 Assessed Maturity
Recover	Contingency Planning	AmeriCorps did not complete the three steps in accomplishing a Business Impact Analysis (BIA) in accordance with NIST SP 800-34 Revision 1 and ensure that a financial management system adheres to the minimum requirements. Additionally, AmeriCorps did not develop a BIA for the ARC Financial System. (*Finding 7*)	Consistently Implemented

Summary of AmeriCorps' Management's Response

AmeriCorps is committed to collaborating with the OIG to address identified risks and enhance the maturity of their cybersecurity framework. AmeriCorps provided comments on the draft FY 2024 FISMA audit report, conducted by RMA Associates, LLC. AmeriCorps' comments are included in their entirety in **Appendix IV**.

Auditor's Evaluation of AmeriCorps Management's Response

We appreciate AmeriCorps' response to the audit findings and recommendations and thank AmeriCorps for its cooperation during the FY 2024 FISMA audit. Overall, we acknowledge AmeriCorps has made improvements and believe its planned corrective actions will resolve issues identified in the report. However, management did not specify the findings and recommendations with which they were in agreement or disagreement. Based on our evaluation of management's response, we have determined our findings, recommendations, and appendices will remain as written.

All recommendations will remain open until AmeriCorps submits documentation to demonstrate the completion and sufficiency of the corrective actions.

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 audit objective, scope, and methodology; **Appendix III** summarizes the status of prior year recommendations; **Appendix IV** captures management's comments on this report and **Appendix V** defines the acronyms used within this report.

RMA Associates

Arlington, VA
November 14, 2024

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

FISMA Audit Findings

Security Function: Identify

1. AmeriCorps Must Improve its Inventory Management Process

FY 2024 IG FISMA Function: *Identify* / **Domain**: *Risk Management*

AmeriCorps did not maintain proper inventory management controls. The inventory list outlining the model type and current state of assets was not accurately documented for all assets. Specifically,

- 73 of 4,466 or 1% of deployed assets were listed as "Default" for Model and Model Category; and
- 302 of 4,466 or 6% of deployed assets (i.e., workstations, computer peripherals, monitors, printers) were listed as "In Use" with no assigned individual when the correct state was "In Stock."

In addition, monthly reviews for correctness were not performed by AmeriCorps to address inaccuracies within the inventory management system.

AmeriCorps' OIT identified errors while importing inventory information into the inventory management system's Configuration Management Database (CMDB). Upon notification, management manually revised the inventory. However, AmeriCorps did not perform the monthly inventory review to ensure the information was complete and accurate as required by AmeriCorps' *Information Technology Managed Systems (ITMS) Asset Tracking Procedures*. The monthly review was initially implemented as a quality assurance measure to identify incomplete or inaccurate inventories.

NIST standards[2] require organizations to develop and document an inventory of information system components that: 1) accurately reflects the current information system and 2) includes all components within the authorization boundary of the information system. The AmeriCorps Cybersecurity Control Families document requires the information system component inventory to be reviewed and updated at least annually.

Furthermore, AmeriCorps' OIT, *ITMS Asset Tracking Procedures* requires that "The Tier 2 lead generates the inventory management system Report – CI Changes for this month on a monthly basis and audit for correctness by spot-checking." In addition, "The Tier 2 lead will meet individually with any techs with errors to correct the inventory management system and reinforce procedure."

[2] NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, CM-8, System Component Inventory control.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

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

We recommend the AmeriCorps' Chief Information Security Officer (CISO):

1) Enforce the requirement for the Tier 2 lead to perform the monthly audit of the inventory report. (**New**)

2. AmeriCorps Must Develop Supply Chain Risk Management Procedures

FY 2024 IG FISMA Function: *Identify* / **Domain**: *Supply Chain Risk Management*

Agencies are required to develop, document, and disseminate procedures to facilitate the implementation of a SCRM policy and the associated SCRM controls. The SCRM strategy and related policies were documented and disseminated; however, the associated procedures to implement the strategy and policies were not documented or disseminated. AmeriCorps did not develop, document, and communicate procedures addressing the following SCRM requirements:

- The identification and prioritization of externally provided systems, system components, and services, as well as how the organization maintains awareness of its upstream suppliers.
- Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers.
- Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third-party providers, as appropriate.
- Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.
- Procedures to detect and prevent counterfeit components from entering the system.
- Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.
- Requirements and procedures for reporting counterfeit system components.

As a result, AmeriCorps does not currently meet the following FISMA SCRM requirements:

- The identification and prioritization of externally provided systems, system components, and services, as well as how the organization maintains awareness of its upstream suppliers.
- Integration of acquisition processes, including the use of contractual agreements that stipulate appropriate cyber and SCRM measures for external providers.
- Tools and techniques to use the acquisition process to protect the supply chain, including, risk-based processes for evaluating cyber supply chain risks associated with third-party providers, as appropriate.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- Contract tools or procurement methods to confirm contractors are meeting their contractual SCRM obligations.

AmeriCorps performed activities related to the remaining three requirements; however, it did not have documented procedures that aligned with these activities:

- Procedures to detect and prevent counterfeit components from entering the system.
- Procedures to maintain configuration control over organizationally defined system components that are awaiting repair and service or repaired components awaiting return to service.
- Requirements and procedures for reporting counterfeit system components.

Executive agencies are required to develop processes to guide and govern SCRM activities.[3] In addition, NIST standards[4] state the enterprise-wide approach to managing cybersecurity risks throughout the supply chain is enacted via enterprise risk management policies, processes, and procedures. Furthermore, NIST standards[5] require agencies to develop, document, and disseminate procedures to facilitate the implementation of the SCRM policy and the associated SCRM controls.

The lack of SCRM procedures may result in the inability to identify and reduce unanticipated supply chain risks. This may increase the potential for disruption and impact the mission's success in terms of malicious adversarial activity and data exfiltration.

We recommend that the AmeriCorps' CISO:

2) Develop, document, and communicate Supply Chain Risk Management procedures to address all FISMA Supply Chain Risk Management requirements. (**Modified Repeat of Recommendation 6 from the FY 2021 evaluation.**)

Security Function: Protect

3. AmeriCorps Must Improve its Vulnerability and Patch Management Controls

FY 2024 IG FISMA Function: *Protect* / **Domain**: *Configuration Management*

Vulnerability management is the ongoing, regular process of identifying, assessing, reporting on, managing and remediating cyber vulnerabilities across endpoints, workloads, and systems. Patch management is both a key component and subset of vulnerability management. It is the process of identifying, acquiring, installing, and verifying patches for products and systems.

[3] P.L. 115-390, 115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act* or the *SECURE Technology Act*, December 21, 2018.
[4] NIST SP 800-161, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*.
[5] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, SR-1, Policy and Procedures.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

To assess the vulnerability and patch management controls, we conducted an independent internal scan for vulnerabilities. We determined a decrease in internal hosts impacted by vulnerabilities within the Internet Protocol addresses provided by AmeriCorps, as compared to the FY 2023 FISMA evaluation.

AmeriCorps has had a long-standing issue with reducing critical and high vulnerabilities in their network. While they have made improvements reducing these vulnerabilities, more work is needed to effectively address them. AmeriCorps management relies heavily on an automated patching process that still requires improvements. Additionally, there was a lack of enforceability in vulnerability remediation as patches from vendors were not always readily available toward remediation efforts and lead to aged vulnerabilities.

Critical and High Vulnerabilities

Our audit identified ongoing challenges for AmeriCorps in promptly addressing vulnerabilities.[6] Specifically, AmeriCorps was delayed in addressing vulnerabilities in certain instances when vendors had not produced the applicable patch or fix necessary for remediation. In addition, internal hosts which were not connected to AmeriCorps' network could not receive patches or fixes.

Approximately 25 percent of the discovered critical and high vulnerabilities were over 12 months old. The longer the vulnerability is exposed on the network, the greater the risk of exploitation. Per AmeriCorps' policies, critical and high vulnerabilities must be mitigated within 15 days and 30 days of identification, respectively. In addition, NIST[7] standards require organizations to resolve their system flaws systematically and improve the security and integrity of their software and firmware. Furthermore, security-relevant updates must be installed within an agency-specified period after release, and flaw remediation is integrated into the organizational configuration management process to ensure proper documentation and tracking fixes.

Ineffective or untimely remediation of vulnerabilities increases the risk that mission information or other sensitive data may be inadvertently or deliberately misused. Such misuse may result in improper information disclosure, manipulation, or theft. Additionally, vulnerabilities that are not corrected may lead to inappropriate or unnecessary changes to mission-focused information systems, which could result in the compromise of mission information or other sensitive data.

Therefore, our prior recommendation remains open. Refer to **Appendix III** for the FY 2019 Recommendation 1. We are not issuing new recommendations related to this finding.

[6] The NIST National Vulnerability Database states that the Common Vulnerability Scoring System (CVSS) provides a standardized scoring system, and the severity of vulnerabilities is categorized into different levels. NIST defines a vulnerability with a CVSS score of 10.0 is classified as critical, indicating that the attacker can easily exploit the vulnerability without significant barriers, and the impact on confidentiality, integrity, and availability is certain. A vulnerability with a CVSS score between 7.0 and 9.9 is classified as high, indicating that the attacker can directly access the vulnerability with minor barriers and the impact on confidentiality, integrity, and availability is likely.

[7] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, SI-2, Flaw Remediation.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Management should continue to take steps to implement Recommendation 1 identified during the FY 2019 FISMA evaluation.

4. AmeriCorps Must Improve Its Personnel Screening Process

FY 2024 IG FISMA Function: *Protect* / **Domain**: Identity and Access Management

The purpose of performing background checks is to ascertain the suitability of an individual for a specific position. Background checks should be conducted before contractors obtain access to AmeriCorps systems. AmeriCorps did not consistently ensure contractors had the proper background investigations prior to granting system access. Specifically, we noted that two out of a sample of five individuals had not undergone an initial background investigation prior to gaining system access. The two individuals are contractors.

OIT did not notify Personnel Security, a subset of the Office of Human Capital, that two new contractors were being onboarded via the Contractor Onboarding System. As a result, Personnel Security did not perform the necessary background investigations before these contractors gained access to AmeriCorps' systems.

NIST standards[8] require organizations to screen individuals prior to authorizing access to the information system.

AmeriCorps guidance[9] requires that all AmeriCorps employees or contractors filling positions that require access to AmeriCorps' facilities, information systems, controlled unclassified information, or other proprietary information are subject to a background investigation to establish suitability/fitness based on the duties assigned.

Though the guidance does not explicitly state that a background investigation is required before system access, it states that under specified circumstances, interim access to facilities and systems may be granted, pending successful completion of the required background investigation. [10] This guidance implies that a background investigation is normally required before system access.

Notwithstanding the guidance, there is a higher risk of allowing individuals with malicious intent or a history of unethical behavior access to AmeriCorps' systems without background checks, leading to potential insider threats. It only takes one incident to result in a security breach. Background checks help ensure that only trustworthy individuals have access to sensitive systems and data, and skipping this step can compromise the organization's overall security posture.

[8] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, PS-3, Personnel Screening.
[9] *Guidance and Procedures for the Personnel Security Program in the AmeriCorps formally known as Corporation for National and Community Service (CNCS)*, Section 8, *Background Investigation Requirements*.
[10] Ibid, page 4.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

We recommend the AmeriCorps' OIT:

3) Develop and implement a written oversight process to ensure that Contracting Officer's Representatives regularly provide the Office of Human Capital with names of contractors who require background investigations and that the Office of Information Technology confirms those background investigations are complete before contractors receive system access. (**New**)

Security Function: Detect

5. AmeriCorps Must Develop the Overdue Authorization to Use Package at the System Level

FY 2024 IG FISMA Function: *Detect* / **Domain**: *Information Security Continuous Monitoring*

An ATU for shared vendor information systems is a critical step in ensuring the security and compliance of an information system. The existence of an ATU signifies that the system has met the required standards and has been authorized to operate within a specific organization. An ATU is employed when an organization (referred to as the customer organization) chooses to accept the information in an existing authorization package produced by another organization (either federal or nonfederal) for an information system authorized to operate by a federal entity (referred to as the provider organization).

During the authorization process, any identified vulnerabilities or weaknesses are addressed through remediation efforts, which may involve implementing additional controls or making necessary configurations. The documentation and assessment findings are then reviewed by the designated authority, which evaluates the system's compliance with security requirements and makes a decision regarding the ATU. If the system is deemed to have met the necessary standards, the ATU is granted.

For the FY 2024 audit, AmeriCorps provided all continuous monitoring reports and authorization to operate (ATO) package documentation for three of the four in-scope systems: a financial management system, eSPAN, and GSS systems. AmeriCorps was in the process of preparing an ATU for the ARC Financial System in response to the prior year's finding, but it was not complete at the time of this audit.

In the past, AmeriCorps relied on government-shared service systems and their ability to maintain parameters established in their existing authorization packages, instead of establishing an ATU package for systems operated by shared service providers within the AmeriCorps environment.

NIST standards[11] state that the ATU is a mechanism to promote reciprocity for systems under the purview of different Authorizing Officials. An ATU is issued by an Authorizing Official from the

[11] NIST 800-37 Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, Appendix F.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

customer organization instead of an ATO. The official issuing an ATU has the same level of responsibility and authority for risk management as an Authorizing Official issuing an ATO or a common control authorization.

In addition, an ATU requires the customer organization to review the authorization package from the provider organization as the fundamental basis for determining risk. The sharing of the authorization package (including security and privacy plans, security and privacy assessment reports, plans of action and milestones, and the authorization decision document) is accomplished under terms and conditions agreed upon by all parties (i.e., the customer organization and the service provider organization). Additionally, per AmeriCorps' *Authorization to Use Process and Procedures*,[12] a shared service, system, and/or application owned, operated by, or on behalf of a federal agency requires an ATU.

Without an ATU for the ARC Financial System, the Authorizing Official and other agency stakeholders may not be aware of security and privacy risks to the systems; potentially impacting the overall risk exposure and compromising the confidentiality, integrity, and availability of AmeriCorps data and information systems.

We recommend that AmeriCorps' CISO:

4) Complete the Authorization To Use package that covers the Administrative Resource Center Financial System. (**Modified Repeat of Recommendation 5 from the FY 2023 evaluation.**)

Security Function: Respond

6. AmeriCorps Must Comply with Logging Requirements

FY 2024 IG FISMA Function: *Respond* / **Domain**: *Incident Response*

AmeriCorps did not meet logging requirements set forth by OMB M-21-31,[13] which requires agencies to reach a tier maturity within 18 months of the M-21-31 memorandum issued on August 27, 2021. Since the issuance of M-21-31, AmeriCorps has not met the specified timeframes to assess maturity levels within 60 days, complete Tier 1 within one year and Tier 2 within 18 months. AmeriCorps has not implemented the requirement to retain logs in acceptable formats since OMB M-21-31 was issued.

AmeriCorps did not meet the logging requirements due to an absence of a detailed project plan addressing the complexity and volume of logging requirements, including log types, log retention periods, and log management. Additionally, AmeriCorps' SIEM was not upgraded and configured to capture all the logs required by OMB M-21-31 and recommended as a result of the FY 2023

[12] Standard Operating Procedures (SOP): *AmeriCorps Authorization to Use Process and Procedure, v1.0.*
[13] OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents*, pages 1-3.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

FISMA evaluation. AmeriCorps utilized a leading SIEM[14] solution to collect, analyze, and correlate security event data from various sources within an IT infrastructure. This SIEM solution has functionalities such as log management, threat detection, incident response, and compliance reporting.

AmeriCorps' failure to meet the logging requirements decreases its ability to ensure the highest-level security operations center and accelerate incident response efforts to enable more effective cybersecurity defense of Federal information.

Therefore, our prior recommendation remains open. Refer to **Appendix III** for the FY 2023 Recommendation 10. Management should continue to take steps to implement Recommendation 10 identified during the FY 2023 FISMA evaluation. In addition, we are issuing one new recommendation related to this finding.

We recommend that AmeriCorps' CISO:

5) Perform a gap analysis by reconciling all Security Information and Event Management solutions that are capturing logs. (**New**)

Security Function: Recover

7. AmeriCorps Must Improve its Contingency Planning Process

FY 2024 IG FISMA Function: *Recover* / **Domain**: *Contingency Planning*

A BIA is used to predict the consequences of a disruption to a business, and it gathers the information needed to develop recovery strategies. Organizations are required by Federal standards and AmeriCorps' policy to develop a Contingency Plan for each information system, in which the BIA's results are incorporated. During our FISMA audit, we observed the following:

1. AmeriCorps did not include the following minimum requirements in the BIA for a financial management system:
   - Identify essential mission/business processes and determine the impact of a system disruption on those processes along with outage impacts and estimated downtime; and
   - Identify recovery priorities for system resources.
2. AmeriCorps did not perform a BIA for the ARC Financial System.

AmeriCorps has not included a government-shared service, ARC Financial System, within its recovery strategy. In the past, AmeriCorps placed reliance on government-shared service systems and their ability to maintain parameters established in its Interagency Agreements, instead of establishing a BIA to include systems operated by shared service providers within the AmeriCorps

[14] SIEM functionality includes log management, threat detection, incident response, and compliance reporting.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

environment. However, Interagency Agreements do not consider the specific circumstances of AmeriCorps or any federal agency that uses their financial services.

NIST standards[15] require organizations to develop a Contingency Plan for each information system, incorporating the BIA's results. BIA results include identifying essential mission and business functions and associated contingency requirements, specifying recovery objectives and restoration priorities, and maintaining essential mission and business functions despite system disruption, compromise, or failure.

Contingency plan testing, including disaster recovery exercises, is critical to confirm the effectiveness of the plans in place. Without effective plans, AmeriCorps' mission data is at a higher risk of loss due to an unscheduled disruption. Specifically, unscheduled disruptions in operations may debilitate AmeriCorps, such that it may be unable to recover and continue operations of all necessary systems and functions in a timely manner.

If a cybersecurity incident that limited access to the ARC Financial System occurred, AmeriCorps would not have the ability to process transactions. AmeriCorps would find itself ill-prepared to implement alternative procedures and determine the appropriate timing for its implementation. Without a comprehensive system-level BIA and contingency plan, there is a heightened risk that the agency may struggle to effectively prioritize recovery operations during a service-impacting incident. An inaccurate BIA for a financial management system that does not meet all minimum requirements can significantly hinder AmeriCorps' ability to respond to and recover from disruptions. It may lead to misaligned recovery prioritization, delays in recovery time, inefficient resource allocation, incomplete recovery strategies, compliance issues, and decreases in the ability to minimize the impact of disruptions on business operations.

Therefore, our prior recommendations remain open. Refer to **Appendix III** for the FY 2023 Recommendations 14 and 15. We are not issuing new recommendations related to this finding. Management should continue to take steps to implement Recommendations 14 and 15 identified during the FY 2023 FISMA evaluation.

[15] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, CP-2, Contingency Plan.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix I – Background

AmeriCorps[16] 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 an inventory of nine information systems – 1) the Network or GSS, 2) eSPAN (which includes the eGrants grants management system), 3) a financial management system, 4) AmeriCorps Health Benefits, 5) AmeriCorps Childcare Benefits System, 6) Treasury Administrative Resource Center, 7) Presidential Volunteer Service Awards, 8) Online Ordering system, and 9) public websites. The first five of these systems are categorized as moderate security applications, while the Online Ordering system and public websites were rated as low security.[17] All eight systems were hosted and operated by third-party service providers, although AmeriCorps hosts certain components of the GSS. AmeriCorps' network consists of multiple sites: Headquarters, eight regional offices, and four National Civilian Community Corps (NCCC) campuses. These facilities were connected through commercially managed telecommunications network connections.

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

The Chief Information Officer (CIO) leads OIT and AmeriCorps' IT operations. AmeriCorps OIT supports AmeriCorps' technology and information needs and project management services during the life cycle of major system acquisitions through daily operations. The CIO is assisted by the CISO, who manages the OIT/Cybersecurity office, which is 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, incorporating NIST SP 800-53, Revision 5.

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

[17] Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*, (February 2004), determines the security category (i.e., low, moderate, high) of a Federal information system based on its confidentiality, integrity, and availability.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix II – Objective, Scope, and Methodology

Objective

The objective of our audit was to determine the effectiveness of AmeriCorps' information security program and practices and report the results to the OMB in accordance with FISMA requirements and NIST guidance.

Scope

We conducted this performance audit in accordance with Generally Accepted Government Auditing Standards (GAGAS). Those standards require that we plan and perform the audit to obtain sufficient, appropriate evidence to provide a reasonable basis for our findings and conclusions based on our audit objective. We believe the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

The overall scope of the FISMA audit was the assessment of relevant information security program and practices to report on the effectiveness of AmeriCorps' Agency-wide information security program for the period of August 1, 2023, through July 31, 2024, in accordance with the OMB's annual FISMA reporting instructions. We audited 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 audit included the testing of select management, technical, and operational controls outlined in NIST SP 800-53, Revision 5 for the following information systems:

- GSS;
- eSPAN;
- ARC; and
- A financial management system.

The audit was conducted remotely from August 1, 2023, through July 31, 2024. A network vulnerability assessment was also conducted at HQ.

The audit also included a follow-up on recommendations from prior years to determine whether AmeriCorps made progress in implementing the recommended improvements concerning its information security program.

Methodology

Following the framework for minimum security controls in NIST SP 800-53, Revision 5, certain controls were selected from NIST security control families associated with the FY 2024 IG FISMA

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Metrics Domains aligned with the Cybersecurity Framework Security Functions. To accomplish the audit objective, we:

- Interviewed key personnel and examined legal and regulatory requirements stipulated by FISMA.
- Examined documentation related to AmeriCorps' information security program, such as security policies and procedures, SSPs, security control assessments, risk assessments, security assessment authorizations, plans 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.
- Evaluated the status of recommendations in the FY 2023 FISMA report, including supporting documentation, to ascertain whether the actions taken addressed the weakness.[18] Refer to **Appendix III** for the status of prior year recommendations.

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

- FIPS PUB 199, *Standards for Security Categorization of Federal Information and Information Systems*
- OMB M-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*
- *FY 2023 – 2024 IG FISMA Reporting Metrics*
- NIST SP 800-161, Revision 1, *Cybersecurity Supply Chain Risk Management Practices for Systems and Organizations*
- NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, for specification of security controls
- NIST SP 800-53A, Revision 5, *Assessing Security and Privacy Controls in Information Systems and Organizations*, for the assessment of security control effectiveness
- NIST SP 800-37, Revision 2, *Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy*, for the risk management framework controls
- NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*
- NIST SP 800-12, Revision 1, *An Introduction to Information Security*
- NIST, *Framework for Improving Critical Infrastructure Cybersecurity*, Version 1.1
- NIST IR 8286D, *Using Business Impact Analysis to Inform Risk Prioritization and Response*
- OMB M-23-16, *Update to Memorandum M-22-18*, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*
- OMB M-22-18, *Enhancing the Security of the Software Supply Chain through Secure Software Development Practices*

[18] *Fiscal Year 2023 Federal Information Security Modernization Act Evaluation of AmeriCorps*, OIG-EV-23-08, September 29, 2023.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- OMB M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incident*
- *Guidance and Procedures for the Personnel Security Program in the AmeriCorps formally known as Corporation for National and Community Service (CNCS)*
- SOP: *AmeriCorps Authorization to Use Process and Procedure*, v1.0
- P.L. 115-390, 115th Congress, *Strengthening and Enhancing Cyber-capabilities by Utilizing Risk Exposure Technology Act* or the *SECURE Technology Act*

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 audit). 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.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix III – Status of Prior Year Recommendations

During FY 2024, AmeriCorps implemented corrective actions to close 19 prior year recommendations from the FY 2017 to FY 2023 FISMA evaluations. Ten recommendations remain open (**Table 4**), in addition to three new FY 2024 recommendations, as mentioned above.

Table 4: Status of Prior Year Recommendations

Recommendation	Auditor Position on Status of Recommendations[19]
FY 2017	
Recommendation 25: Ensure the AmeriCorps GSS Information System Owner establishes and enforces the policy for mobile devices that do not connect to the AmeriCorps GSS to include usage restrictions, configuration, and connection requirements, and implementation guidance.	Closed RMA testing determined that the recommendation 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 reimage 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 AmeriCorps-issued email accounts. • Configure cell phones to require the enabling of security functions.	Closed RMA testing determined that the recommendation was implemented.

[19] Status as of August 31, 2024.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Recommendation	Auditor Position on Status of Recommendations[19]
FY 2019	
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 the 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 RMA testing determined the recommendation remains open. See Finding 3: AmeriCorps Must Improve its Vulnerability and Patch Management Controls.
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.	Open AmeriCorps has implemented sufficient network allowance for 3 of the 4 NCCC campus locations to handle scanning, patching, and network monitoring. The remaining NCCC Campus is in process. Additionally, AmeriCorps is working on the plan and implementation for the Regional Offices.
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 RMA testing determined that the recommendation was implemented.
Recommendation 6: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.	Open RMA will assess this recommendation in FY25.
Recommendation 7: Perform and document analysis to determine the feasibility of completely automating the inventory management process.	Closed RMA determined that this recommendation should be closed as the recommendation is written to the *Optimized* maturity level of the Risk Management domain metric question #2 and is not a practical recommendation.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Recommendation	Auditor Position on Status of Recommendations[19]
Recommendation 23: Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Open RMA will assess this recommendation in FY25.
Recommendation 25: Document and implement a process to validate that physical counselor files from the NCCC Southwest Region Campus are disposed of within six years after the date of the member's graduation in accordance with the AmeriCorps NCCC Manual.	Open RMA will assess this recommendation in FY25.
FY 2020	
Recommendation 4: Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 9: Ensure all personnel whose responsibilities include access to PII complete annual privacy-role-based training.	Closed RMA testing determined that the recommendation was implemented.
FY 2021	
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.	Closed RMA testing determined that the recommendation was implemented.
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 state and indicate who, if anyone, must approve exceptions.	Open AmeriCorps stated they were in the process of addressing the recommendation. Please note, the language of this recommendation was modified to reflect the work conducted by AmeriCorps during this audit period. See Finding 2: AmeriCorps Must Develop Supply Chain Risk Management Procedures.
FY 2022	
Recommendation 6: AmeriCorps enhance its process of performing enterprise risk management assessments to determine the respective risk posture of its systems to include the entity-wide performance metrics for measuring the effectiveness of its: • Data exfiltration and enhanced network defenses; • Incidence detection and analysis process; and • Incidence handling process.	Closed RMA testing determined that the recommendation was implemented.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Recommendation	Auditor Position on Status of Recommendations[19]
FY 2023	
Recommendation 1: Update AmeriCorps' Information System Inventory to include external vendor systems such as Administrative Resource Center Financial System.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 2: Establish policies and procedures to perform an annual review of the inventory to ensure AmeriCorps' Information System Inventory includes all information systems used or operated by an agency, an agency contractor, or another organization on behalf of an agency.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 3: Upgrade to a supported version of the application software and revise the references to the supported software in the Business Impact Analysis or accept the risk of not updating the software by documenting the exposure risk in a formal risk acceptance memo signed by the Authorizing Official.	Closed AmeriCorps is actively managing the risk associated with this software. The expected sunset date is December 2024.
Recommendation 4: Develop and implement an effective monitoring mechanism to track the progress of Authorization to Operate letters within the three-year review window and ensure timely approval of the System Security Plans.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 5: Complete an authorization package that covers the Administrative Resource Center Financial System.	Open RMA testing determined that the recommendation remained open. Please note, the language of this recommendation was modified to reflect the work conducted by AmeriCorps during this audit period. See Finding 5: AmeriCorps Must Develop the Overdue Authorization to Use Package at the System Level.
Recommendation 6: Enhance and implement core and specialized training to develop competencies in authorization packages for external vendor systems such as Administrative Resource Center Financial System.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 7: Finalize and issue the Incident Response Plan for FY 2023.	Closed RMA testing determined that the recommendation was implemented.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Recommendation	Auditor Position on Status of Recommendations[19]
Recommendation 8: Establish and implement a process and an effective monitoring mechanism to track the progress of Incident Response Plan annual reviews ensuring timely completion and updates, adapting the evolving cybersecurity threats, maintaining effective response capabilities, and reflecting the current agency operations and system environment.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 9: Develop a comprehensive project plan and roadmap to meet the logging requirements in accordance with OMB M-21-31.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 10: Upgrade and configure its Security Information and Event Management tool to capture all log requirements in accordance with OMB M-21-31.	Open RMA testing determined that the recommendation remains open. See Finding 6: AmeriCorps Must Comply with Logging Requirements.
Recommendation 11: Implement a tool to closely track the timely completion and review of an annual Disaster Recovery Exercise/Contingency Plan Test conducted to account for all information systems.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 12: Develop and implement standard operating procedures for Disaster Recovery Exercise/Contingency Plan Test coverage of external vendors systems including Administrative Resource Center Financial System.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 13: Enhance and implement core and specialized training programs targeted at the Authorizing Official, System Owner, and Information System Security Officer to develop competencies in contingency planning for external vendor systems.	Closed RMA testing determined that the recommendation was implemented.
Recommendation 14: Complete the three steps in accomplishing Business Impact Analysis in accordance with NIST SP 800-34, Revision 1 and ensure the application adheres to the minimum requirements.	Open RMA testing determined that the recommendation remains open. See Finding 7: AmeriCorps Must Improve its Contingency Planning Process.
Recommendation 15: Develop a Business Impact Analysis for Administrative Resource Center Financial System.	Open RMA testing determined that the recommendation remains open. See Finding 7: AmeriCorps Must Improve its Contingency Planning Process.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix IV – Management's Response

AmeriCorps

November 01, 2024

To: Tamekia Anglin, Audit Manager

From: Prabhjot Bajwa, Chief Information Officer

Re: AmeriCorps management response to Report Number: OIG-AR-24-03 FY 2024 Federal Information Security Modernization Act (FISMA) Audit

This memorandum provides AmeriCorps' response to the Office of Inspector General (OIG) draft report on the FY 2024 Federal Information Security Modernization Act (FISMA) Evaluation, issued on October 18, 2024.

AmeriCorps values the OIG's annual FISMA audit as essential to our cybersecurity program improvement efforts. The recommendations and feedback provided have helped strengthen our security posture, and we remain committed to collaborating with the OIG to address identified risks and enhance the maturity of our cybersecurity framework.

We concur with most of the findings and appreciate the time and effort invested by the OIG in this process. The risk-based approach taken by the OIG continues to help identify areas for improvement, and we are fully dedicated to addressing them. In FY 2024, AmeriCorps made significant strides in advancing our cybersecurity program, including:

- Enforcing AmeriCorps usage restrictions, configuration, and connection requirements on mobile devices that do not connect to AmeriCorps General Support System.
- Consolidated Configuration Management Database inventory for all AmeriCorps assets, including National Civilian Community Corps campuses (NCCC).
- Implemented a process for scanning approved deviations for standard baseline configurations.
- Ensured all personnel whose responsibilities include access to PII completed annual privacy role-based training.
- Designed and implemented effective accountability identifying clear expectations of goals, performance measures, and target dates for OIT leadership responsible for improving AmeriCorps information security program to an effective level.
- Enhanced the process in which enterprise risk management assessments determining the risk posture of its systems to include performance metrics.
- Updated our Information System Inventory to include external vendor systems and established policies and procedures to perform annual reviews.
- Completed Business Impact Analysis and Risk Acceptance providing clarification for not upgrading and supporting continued use of current software version.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- Developed and provided specialized training for authorization packages, incident response, and contingency planning.
- Developed and executed comprehensive incident response testing and contingency plan testing for all information systems.
- Developed a comprehensive project plan and roadmap to meet logging requirements in accordance with OMB M-21-31 and have already initiated the implementation process.

AmeriCorps remains enthusiastic about the security program improvements achieved through our partnership with the OIG and looks forward to continuing this collaboration. During our review of the OIG-AR-24-03 Draft Report, we have identified several questions, recommendations, and points of clarification. The sections of the Draft Report and our corresponding comments are listed below.

Vulnerability and Patch Management Controls

- While we agree that patch management needs to be improved to enhance the effectiveness of future assessments, we'd like to ensure that the established Rules of Engagement are adhered to throughout the process. We didn't receive access to the raw Nessus data, which made it a bit challenging for us to conduct a comprehensive analysis. More effective communications in the future would support success.

Personnel Screening Process

- We are enhancing our access provision form and coordinating with relevant offices to ensure preconditions are met before granting system access.

Logging Requirements

- Clarifying the specific tier referenced in the report regarding compliance with OMB M-21-31 would be appreciated.

Appendix I – Background

There seems to be an oversight related to the count of information systems reported within AmeriCorps. On February 13, 2024, the auditors were provided with the AmeriCorps System Inventory, which contained 30 Information Systems.

Recommendations

- FY 2019 Recommendation 6: This recommendation referred to developing a process for reconciling the CMDB with the FasseTrack system. However, as noted in our June 27 and August 2, 2024, communications, FasseTrack is no longer in use as of April 22, 2024, and we now track NCCC assets exclusively through ServiceNow. We also monitor these assets within CDM. Given that Recommendation 4 (regarding manual updates to CMDB) was closed on the same basis, we believe Recommendation 6 should be considered resolved as well. Supporting documentation was provided in the FY19 closure package under FY19-CNS-2.4 and FY19-CNS-2.6 to the auditors.

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

- FY 2019 Recommendations 23 and 25: While the June 7, 2024, follow-up items spreadsheet did not include these recommendations, both were addressed through AmeriCorps' Corrective Action Plan. The supporting closure artifacts were provided internally on November 11, 2023. Since neither recommendation was mentioned in the audit discussions or included in the July 26, 2024, NFR email, their presence in the draft report as "still in process" appears to be an oversight. We kindly request these be marked as not reviewed.

Cyberscope Submission

- Lastly, we request that the final report include the 2024 FISMA Annual IG audit submission from Cyberscope as an appendix.

We look forward to continued collaboration as we value the annual audit to inform and improve AmeriCorps' cybersecurity posture.

PRABHJOT BAJWA
Digitally signed by PRABHJOT BAJWA
Date: 2024.11.01 22:47:23 -04'00'

Yours sincerely,

Prabhjot Bajwa

Chief Information Officer

4121 Wilson Blvd., Suite 1110
Arlington, VA 22203
Phone: (571) 429-6600
www.rmafed.com

Appendix V – Acronym List

Acronym	Description
ARC	Administrative Resource Center
ATO	Authorization to Operate
ATU	Authorization to Use
BIA	Business Impact Analysis
CIO	Chief Information Officer
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CNCS	Corporation for National and Community Service
CVSS	Common Vulnerability Scoring System
eSPAN	Electronic-System for Programs, Agreements and National Service
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAGAS	Generally Accepted Government Auditing Standards
GSS	General Support System
IT	Information Technology
ITMS	Information Technology Managed Systems
NCCC	National Civilian Community Corps
NFR	Notice of Findings and Recommendations
NIST	National Institute of Standards and Technology
OIG	Office of Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
P.L.	Public Law
PII	Personally Identifiable Information
RMA	RMA Associates, LLC
SCRM	Supply Chain Risk Management
SIEM	Security Information and Event Management
SOP	Standard Operating Procedures
SP	Special Publication

AmeriCorps
Office of Inspector General

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

OFFICE OF INSPECTOR GENERAL
HOTLINE: 1.800.452.8210
AmeriCorpsoig.gov/hotline | AmeriCorpsOIG.gov