AmeriCorps

OFFICE OF INSPECTOR GENERAL

FISCAL YEAR 2023 FEDERAL INFORMATION SECURITY MODERNIZATION ACT EVALUATION OF AMERICORPS

FINAL AUDIT REPORT

NUMBER: OIG-EV-23-08

September 29, 2023

OFFICE OF INSPECTOR GENERAL
AmeriCorps

OFFICE OF INSPECTOR GENERAL
AmeriCorps

September 29, 2023

MEMORANDUM TO: Prabhjot Bajwa
Chief Information Officer

FROM: Monique P. Colter *Monique P. Colter*
Assistant Inspector General for Audit

SUBJECT: Fiscal Year 2023 Federal Information Security Modernization Act Evaluation of AmeriCorps (OIG Report- EV-23-08)

Enclosed is the AmeriCorps Office of Inspector General (OIG) final report on the Fiscal Year 2023 Federal Information Security Modernization Act (FISMA) Evaluation of AmeriCorps, OIG Report EV-23-08.

The OIG contracted with the independent certified public accounting firm of RMA Associates, LLC (RMA) to conduct the FISMA evaluation for Fiscal Year (FY) 2023. 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 *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) 606-9360 or m.colter@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
Fernando Laguarda, General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits and Investigations Program Manager
Heather Leinenbach, Assistant to the Board of Directors
Stephen Ravas, Acting Inspector General
George Fallon, Principal, RMA Associates, LLC

RMA Associates
Auditors. Consultants. Advisors.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

AmeriCorps

Federal Information Security Modernization Act Evaluation Report

Fiscal Year 2023

September 29, 2023

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Table of Contents

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Executive Summary

Introduction

The Federal Information Security Modernization Act of 2014 (FISMA)[1] requires Federal agencies to have an annual independent evaluation 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 evaluation for Fiscal Year (FY) 2023.

The objective of this evaluation was to determine the effectiveness of AmeriCorps' information security program and practices for the period October 1, 2022, through July 31, 2023, and report the results to the Office of Management and Budget (OMB). This report presents the results of RMA's independent evaluation of AmeriCorps' information security program and practices in accordance with FISMA. The evaluation 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
- An application.

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: Inspector General (IG) Evaluation Maturity Levels** 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.

Table 1: IG Evaluation 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.

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

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Maturity Level	Maturity Level Description
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.

Evaluation Results

We assessed AmeriCorps' overall maturity level as *Consistently Implemented* (Level 3), **not effective,** for the period of October 1, 2022 through July 31, 2023. We determined AmeriCorps' control processes were operational and generated information that supported control monitoring and decision-making. We also identified seven weaknesses in AmeriCorps' control processes that hindered the effectiveness of the overall information security program. AmeriCorps must implement further internal controls including implementing 14 prior year recommendations that remain open to reach 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' maturity and effectiveness levels have increased from the prior year and are presented in **Table 2: FY 2022 – FY 2023 Maturity Level Comparison.**

Table 2: FY 2022 – FY 2023 Maturity Level Comparison

Function	FY 2022 Maturity	FY 2023 Maturity
Identify	Defined	Consistently Implemented
Protect	Defined	Consistently Implemented
Detect	Defined	Defined
Respond	Consistently Implemented	Consistently Implemented
Recover	Managed and Measurable	Defined
Overall Maturity	Defined	Consistently Implemented
Overall Effectiveness	**Not Effective**	**Not Effective**

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

AmeriCorps made progress in implementing prior recommendations; however, further improvements in information security are needed for the program to be rated effective. During FY 2023, AmeriCorps resolved 19 of 33 open recommendations from prior year evaluations, yielding slight improvements in the IG FISMA Metrics results. To address the continuing weaknesses in AmeriCorps' information security program and practices, we identified 15 new recommendations in addition to 14 prior year recommendations that remain open. See **Appendix III – Status of Prior Year Recommendations** 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. Vulnerability and Patch Management Program;
3. Unsupported Software;
4. Authorization Packages;
5. Incident Response Plan;
6. Logging;
7. Contingency Planning Process.

These control weaknesses directly affected the maturity levels of the functional areas of information security, as shown in **Table 3: FY 2023 Function Area Control Weaknesses**.

Table 3: FY 2023 Function Area Control Weaknesses

Function	Domain	Control Weakness	FY 2023 Assessed Maturity
Identify	Risk Management, Supply Chain Risk Management	AmeriCorps did not maintain a complete and accurate inventory of all its information systems. In addition, AmeriCorps did not maintain proper inventory management controls. (*Finding 1)* AmeriCorps has not defined and communicated its policies, procedures, and processes to ensure the organization adheres to its cybersecurity and supply chain risk management requirements. (*Recommendation 6 – Report Number: OIG-EV-22-03*)	Consistently Implemented

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Function	Domain	Control Weakness	FY 2023 Assessed Maturity
Protect	Configuration Management, Identity, and Access Management, Data Protection and Privacy, Security Training	Vulnerabilities related to patch management, configuration management, and unsupported software continue to expose AmeriCorps' network to critical and high-severity vulnerabilities. (*Finding 2*) AmeriCorps used unsupported software, which ended support in 2020. (*Finding 3*)	Consistently Implemented
Detect	Information Security Continuous Monitoring	AmeriCorps did not consistently perform and document security control assessments, risk assessments, and issue an Authorization To Operate (ATO) or Authorization To Use (ATU) for AmeriCorps systems in line with its policies and procedures. (*Finding 4*)	Defined
Respond	Incident Response	AmeriCorps did not annually review and update its enterprise-wide Incident Response Plan defined within the AmeriCorps Security Controls Catalog. (*Finding 5*) AmeriCorps did not meet the logging requirements required by OMB. (*Finding 6*)	Consistently Implemented
Recover	Contingency Planning	AmeriCorps did not perform a Business Impact Analysis for its external vendor systems. (*Finding 7*) AmeriCorps did not conduct a Disaster Recover Exercise for all systems in accordance with its policies and procedures. (*Finding 7*)	Defined

Summary of Management's Comments

AmeriCorps concurred with all findings and recommendations. AmeriCorps valued OIG's recommendations and noted the OIG findings and recommendations were actionable and risk-based. AmeriCorps stated that it is committed to remediating cybersecurity risks, continuing to

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

work diligently to strengthen its enterprise-wide cybersecurity program's maturity, and elevating cybersecurity maturity across all FISMA Evaluation domains.

AmeriCorps will continue to focus on improving its cybersecurity program by developing actionable project plans and corrective action plans, particularly in areas such as information system inventory, disaster recovery efforts, vulnerability and patch management controls, authorization packages, cybersecurity policies, unsupported software, business impact analysis, and logging capabilities. We will evaluate AmeriCorps' corrective actions addressing current and prior year recommendations in the FY 2024 FISMA evaluation.

AmeriCorps' comments are included in their entirety in **Appendix IV– Management's Comments.**

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

RMA Associates

Arlington, VA
September 29, 2023

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

FISMA Evaluation Findings

Security Function: Identify

1. AmeriCorps Must Improve its Information System Inventory Management Process

FY 2023 IG FISMA Function: *Identify* / **Domain**: *Risk Management*

AmeriCorps did not maintain a complete and accurate inventory of all its information systems. During fieldwork, AmeriCorps provided its Information System Inventory List, and we observed one system, the Administrative Resource Center (ARC) Financial System, was not maintained as part of the information system inventory.

AmeriCorps' focus on systems operated and managed directly by its employees has placed less attention on the systems provided as a service. Therefore, AmeriCorps has not consistently captured the level of detail necessary to maintain all systems within its comprehensive information system inventory.

OMB Circular No. A-130, *Managing Information as a Strategic Resource,*[2] defines Federal information system as an information system that is utilized or controlled by a government agency, or by a contractor or another organization acting on behalf of an agency. Furthermore, OMB Circular No. A-130 mandates that Federal agencies have certain obligations when it comes to overseeing information systems used on behalf of the Federal Government or handling Federal information. Specifically, Federal agencies are required to include these information systems in their inventory of information systems to ensure effective tracking and management.

The absence of a complete and accurate inventory of all information systems creates a risk that AmeriCorps (1) may not be aware of all systems in its environment and (2) may not be able to identify and address all existing vulnerabilities. Further, there is an increased risk that unapproved systems may be utilized and process agency information.

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

1) Update AmeriCorps' Information System Inventory to include external vendor systems such as Administrative Resource Center Financial System. (**New**)
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. (**New**)

[2] Circular No. A-130, *Managing Information as a Strategic Resource,* Appendix I, page Appendix I-14.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Security Function: Protect

2. AmeriCorps Must Improve its Vulnerability and Patch Management Controls

FY 2023 IG FISMA Function: *Protect* / **Domain**: *Configuration Management*

Patch management is identifying, acquiring, installing, and verifying patches for products and systems and is a vital component of vulnerability management. We conducted an independent internal scan for vulnerabilities. We determined a decrease of internal hosts impacted by vulnerabilities within the Internet Protocol addresses provided by AmeriCorps, as compared to FY 2022 FISMA evaluation. Despite the decrease, vulnerabilities increased, which can be attributed to both the increased use of credential scans, which probe deeper into software, and the reclassification of a previously low-risk vulnerability as a higher-risk one. Also, we identified more improvements needed to AmeriCorps' patch management, software management, and detection of vulnerabilities.

Critical and High Vulnerabilities

Our evaluation identified delays in applying patches and fixes for critical and high-severity vulnerabilities[3]. Approximately 24 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 that the vulnerability can be exploited. Per AmeriCorps policies, critical and high-severity vulnerabilities must be mitigated in 15 and 30 days, respectively. In addition, NIST[4] requires organizations to resolve their system flaws systematically and improve the security and integrity of their software and firmware. It involves testing updates related to flaw remediation for effectiveness and potential side effects before installation. In addition, security-relevant updates must be installed within a specified time period after release, and flaw remediation is integrated into the organizational configuration management process to ensure proper documentation and tracking of fixes. Ineffective remediation of vulnerabilities increases the risk that mission information or other sensitive data may be inadvertently or deliberately misused.

AmeriCorps had a plan in place to patch and resolve critical vulnerabilities relating to out-of-date Windows operating systems. However, this resolution relied mainly on IT service members manually updating devices, with many employees working remotely, which hindered this progress. There was a lack of oversight and enforceability of the vulnerability remediation, resulting in a lack of timely remediation.

There are currently recommendations open related to the improvement of the vulnerability management program at AmeriCorps. Therefore, we are not issuing any new recommendations

[3] The NIST National Vulnerability Database states that the 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 considered critical, indicating that the attacker can easily exploit the vulnerability without significant barriers, and the impact on confidentiality, integrity, and availability (CIA) 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 CIA is likely.
[4] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, Page 333.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

related to this finding. Management should continue to take steps to implement recommendations 1 and 2 that we identified during our FY 2019 FISMA evaluation.

Refer to **Appendix III – Status of Prior Year Recommendations** for the status of FY 2019 Recommendations 1 and 2.

3. AmeriCorps Must Remove its Unsupported Software

FY 2023 IG FISMA Function: *Protect* / **Domain**: *Configuration Management*

Support for system components includes software patches, firmware updates, replacement parts, and maintenance contracts. An example of unsupported components includes when vendors no longer provide critical software patches or product updates, which can result in an opportunity for adversaries to exploit weaknesses in the installed components. Exceptions to replacing unsupported system components include systems that provide critical mission or business capabilities where newer technologies are not available or where the systems are so isolated that installing replacement components is not an option.

For one out of four selected systems, we determined the FY 2023 Business Impact Analysis (BIA) included unsupported software. The support for this software version ended on March 1, 2020. However, the software continues to provide business capabilities to AmeriCorps' operation, which is critical because it contains AmeriCorps' transactions.

NIST standards[5] require the replacement of unsupported components, which can result in opportunities for adversaries to exploit weaknesses when vendors no longer provide critical software patches or product updates. Additionally, NIST SP 800-40, Revision 4, *Guide to Enterprise Patch Management Technologies* emphasizes the importance of upgrading the software to the latest version to eliminate the organizations' vulnerabilities. Further, OMB Circular No. A-130, Appendix I establishes minimum requirements for Federal information security programs and assigns Federal agency responsibilities for the security of information and information systems. The Circular specifically prohibits Federal Agencies from using unsupported information systems and system components. It requires Federal Agencies to ensure systems and components that cannot be appropriately protected or secured are given high priority for upgrade or replacement. In addition, it requires Federal Agencies to implement and maintain current updates and patches for all software and firmware components of information systems.

AmeriCorps was aware that the unsupported software was in the process of an overall modernization effort to replace the systems. AmeriCorps stated steps have been taken to decommission this system in December of 2024. However, AmeriCorps' plan to decommission the

[5] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* Page 290.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

software at the end of 2024 will risk exposure to unsupported software for fourteen to sixteen months.

Not replacing the unsupported software before the end of life increases the risk that mission-critical information or other sensitive data may be inadvertently or deliberately misused. Such misuse may result in improper information disclosure, manipulation, or theft. Further, unsupported software and uncorrected vulnerabilities may lead to inappropriate or unnecessary changes to mission-focused information systems, resulting in compromising mission-critical information or other sensitive data.

We recommend the AmeriCorps Chief Information Security Officer:

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. **(New)**

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Security Function: Detect

4. AmeriCorps Must Review and Update its Absent and Overdue Authorization Package at System Level.

FY 2023 IG FISMA Function: *Detect* / **Domain**: *Information Security Continuous Monitoring*

Authorization is a critical step in ensuring the security and compliance of an information system. The authorization process includes an Authorization To Operate (ATO) and Authorization To Use (ATU). The ATO provides the authorization to operate the in-house system because it has met the required standards within a specific organization. Whereas the ATU provides the authorization to use cloud and shared systems, services, and applications within a specific organization. An ATO or ATU requires a system to undergo a thorough assessment, which includes evaluating its security controls, policies, and procedures.

During the 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 ATO and ATU. When the system is deemed to have met the necessary standards, the applicable authorization is granted.

During our FISMA evaluation, AmeriCorps:

- Did not update its ATO documentation in accordance with its policies. Specifically, an application and Electronic-System for Programs Agreements and National Service Participant (eSPAN) ATO letters were not updated within three years in accordance with AmeriCorps policies and procedures.
- Did not authorize the System Security Plans (SSP) for an application, eSPAN, and General Support System (GSS). The SSPs were marked draft and without the approval signatures.
- Was unaware they needed to account for third-party systems and prepare an authorization package, including SSPs, ATU, and Security Assessment Report (SAR) for the ARC Financial System.

On June 23, 2023, AmeriCorps provided updated documents for the application ATO letter and approved SSPs after we notified management of the findings on June 15, 2023. On July 11, 2023, AmeriCorps provided the eSPAN ATO letter dated July 7, 2023; however, it was still under the review and approval process with no signatures from the System Owner (SO), CISO, and Authorizing Official (AO).

Table 4: SSP, SAR, and Authorization Status in FY 2023 AmeriCorps FISMA Evaluation provides a detailed breakdown of the initial and updated document review dates mentioned above.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Table 4: SSP, SAR, and Authorization Status in FY 2023 AmeriCorps FISMA Evaluation

System	RMA's Evaluation Date	Required Document	Document's Last Review Date	Document's New Update Date	Days Since Last Review	Years Since Last Review
ARC	5/26/2023	ATU Letter SAR SSP	No document was provided.	No document was provided.	N/A	
An application	5/26/2023	ATO Letter	7/1/2019	6/23/2023	1,457	3yr 11m
		SSP	2/15/2023 (No approval signatures)	6/28/2023	133	0.4yr
eSPAN	5/26/2023	ATO Letter	5/30/2019	7/7/2023 (No approval signatures)	1,489	4yr
		SSP	12/22/2022 (No approval signatures)	6/27/2023	187	0.5 yr
GSS	5/26/2023	SSP	4/8/2022 (No approval signatures)	6/26/2023	444	1yr 3m

The *AmeriCorps Security Controls Catalog* contains organization-defined responses within each control description. Control CA-6 Authorization specifies the necessary steps for assigning authorizing officials for a system and its common controls and requires the authorization to be updated every three years. Under the PL-2 System Security and Privacy Plans Control, security and privacy plans must be developed for the system. Before implementation, the authorizing official or their designated representative must review and approve these plans. The plans should be periodically reviewed and updated to address system and environmental changes, or any problems identified during implementation or control assessments.

Additionally, per AmeriCorps' Procedures[6], the security authorization package contains several crucial documents, which include the SSP, SAR, Plan of Action and Milestones, and an executive summary for the authorization process. These documents are essential for authorizing systems, particularly the use of third-party systems or the operation of systems on-premises. In cases where external providers are responsible for providing controls (e.g., through contracts, interagency agreements, lines of business arrangements, licensing agreements, and/or supply chain arrangements), AmeriCorps should ensure that all relevant information is obtained from the external provider. The AO uses information obtained to make a risk-based decision on whether to authorize the system for use. Furthermore, the security authorization package can include additional information upon request of the AO, CISO, Information Owner, or SO. NIST Standards[7] state that the AO is a senior (Federal) official or executive who possesses the authority to assume formal responsibility for operating a system at an acceptable level of risk to organizational

[6] Standard Operating Procedure (SOP): CS0102 v4.0, titled *Cybersecurity: Security Assessment & Authorization*
[7] NIST SP 800-12, Revision 1, *An Introduction to Information Security*

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

operations (including mission, functions, image, or reputation), organizational assets, individuals, other organizations, and the Nation.

AmeriCorps officials did not start the application, GSS, and eSPAN systems assessments timely, resulting in incomplete assessments during the FY 2023 evaluation period. The delay affected AmeriCorps' ability to produce finalized SSPs for the application, GSS, and eSPAN systems. In addition, AmeriCorps did not have an effective process and monitoring mechanism to track the progress of ATO letters, which delayed the ATO packages for the application and eSPAN systems beyond the three-year coverage period. The GSS's ATO was still within the three-year coverage period once the last review occurred on 5/26/2023, as presented in the table above.

In addition, AmeriCorps officials were also unaware of their responsibility to develop an authorization package for ARC, a shared service provider managed by the Department of Treasury. AmeriCorps incorrectly stated that ARC was outside the authorization boundary because the ARC authorization would be covered within the application SSP. However, the database referred to within the application was not the database used by ARC, the shared service provided.

Without consistently (1) approving the SSPs and (2) reviewing and documenting ongoing authorization for AmeriCorps systems, the AO and other agency stakeholders may not be aware of security and privacy risks to the systems. Specifically, potentially impacting the overall risk exposure to the compromise of confidentiality, integrity, and availability of AmeriCorps data and information systems.

We recommend the AmeriCorps Chief Information Security Officer:

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. (**New**)
5) Complete an authorization package that covers the Administrative Resource Center Financial System (**New**)
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. (**New**)

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Security Function: Respond

5. AmeriCorps Must Review and Update its Incident Response Plan

FY 2023 IG FISMA Function: *Respond* / **Domain**: *Incident Response*

AmeriCorps did not annually review and update its enterprise-wide Incident Response Plan (IRP) as defined within the *AmeriCorps Security Controls Catalog.* During the evaluation, AmeriCorps provided an IRP dated May 5, 2021, and no updates have been made to the document since April 2021. AmeriCorps Officials stated that the most recent version of the IRP was under review and was presented at the AmeriCorps Policy Council Meeting on June 21, 2023.

The absence of oversight by the assigned parties led to a lapse in the reviews and periodic updates of the enterprise-wide IRP within the timeframe defined by the *AmeriCorps Security Control Catalog*. AmeriCorps did not have a process and monitoring mechanism in place to oversee the annual reviews of the IRP.

AmeriCorps Policies and NIST Standards[8] require AmeriCorps to develop, distribute, update, communicate, and protect its IRP, which is reviewed and approved annually. According to the *AmeriCorps Security Control Catalog (Incident Response (IR)-01 & IR-08),* the CISO is designated to manage developing, documenting, and disseminating incident response policies and procedures. The policies and procedures must be reviewed and updated annually and after major events. Establishing an IRP is required to cover various aspects such as structure, unique requirements, metrics, and incident information sharing. The plan should be reviewed and approved at least annually by the CISO and Chief Privacy Officer, and it should explicitly designate responsible roles.

Additionally, organizations must develop and document an incident response policy and procedures per the NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*. Procedures should also be established to facilitate the implementation of the policy and associated incident response controls. The policy and procedures need to be regularly reviewed and updated. In addition, NIST SP 800-53, Revision 5 emphasizes the development of an incident response plan that serves as a roadmap for implementing the organization's incident response capability. The plan should outline the structure, organization, and high-level approach of the incident response capability within the organization. The plan must be reviewed, approved, and distributed to relevant personnel and organizational elements. It also must be protected from unauthorized disclosure and modification.

An outdated or inaccurate IRP increased the risk that AmeriCorps was vulnerable to the escalating threats of cyber-attacks, data breaches, and other emergencies, compromising its security and stability. Therefore, AmeriCorps would be unable to prepare to handle and mitigate incidents, leading to increased damage, prolonged downtime, and disrupted operations.

[8] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations*, IR-8, Page 158-159

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

We recommend the AmeriCorps Chief Information Security Officer:

7) Finalize and issue the Incident Response Plan for FY 2023. (**New**)
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. (**New**)

6. AmeriCorps Must Comply with Logging Requirements

FY 2023 IG FISMA Function: *Respond* / **Domain**: *Incident Response*

OMB Memorandum M-21-31 *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* outlines the requirements for each tier and their corresponding ratings of Log Management.

AmeriCorps did not meet the logging requirements set forth by the OMB M-21-31, which requires agencies to reach a tier maturity within 18 months of the M-21-31 memorandum issued on August 27, 2021. As of June 27, 2023, or 22 months since issuance, 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' Security Information and Event Management (SIEM) was not upgraded and configured to capture all the logs required by OMB M-21-31. AmeriCorps utilized a leading SIEM[9] solution to collect, analyze, and correlate security data from various sources within an IT infrastructure. However, the implementation of the SIEM was inconsistently documented and did not reflect the necessary level of detail encompassing pertinent information. AmeriCorps is planning a license upgrade to continue enhancing its SIEM to meet logging requirements set forth by OMB M-21-31.

AmeriCorps' failure to meet the logging requirements hinders its ability to maintain a top-tier security operations center and accelerates incident response efforts. Subsequently, it affects its ability to enhance cybersecurity defenses for Federal information.

We recommend the AmeriCorps Chief Information Security Officer:

9) Develop a comprehensive project plan and roadmap to meet the logging requirements in accordance with OMB M-21-31. (**New**)
10) Upgrade and configure its Security Information and Event Management tool to capture all log requirements in accordance with OMB M-21-31. **(New)**

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

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Security Function: Recover

7. AmeriCorps Must Improve its Contingency Planning Process

FY 2023 IG FISMA Function: *Recover* / **Domain**: *Contingency Planning*

Disaster Recovery Exercise is a critical element of a feasible contingency capability. The exercise enables plan deficiencies to be identified, ensures their resilience in the face of potential disasters, and ultimately reduces the impact of disruptions on business operations. Additionally, the Business Impact Analysis (BIA) is a key step in implementing the Contingency Planning (CP) controls in NIST SP 800-53, Revision 5, and the overall contingency planning process. The purpose of the BIA is to correlate the system with the critical mission/business processes and services provided and based on that information, characterize the consequences of a disruption.

During our FISMA Evaluation, we observed the following:

1. AmeriCorps did not conduct the Disaster Recovery Exercise for four systems, GSS/eSPAN, an application, and ARC Financial System, in FY 2023.
   - The last exercise was conducted for the GSS and eSPAN systems from October 2021 to November 2021.
   - The last exercise for the application system was conducted in May 2022.
   - The ARC Financial System was not included in the previous year's Disaster Recovery exercises or the FY 2023 exercise.
2. AmeriCorps did not include the minimum requirements for its application BIA to:
   - 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.
3. AmeriCorps did not perform a contingency plan and BIA for the ARC Financial System.

AmeriCorps' CP controls were ineffective due to the following:

- AmeriCorps did not implement the necessary oversight and/or enforcement mechanisms and controls to ensure the Disaster Recovery Exercise/Contingency Plan Test was conducted and results were reviewed to develop corrective actions, as needed, to strengthen the effectiveness of the plans.
- AmeriCorps did not have a standard operating procedure to instruct its employees to perform the annual Disaster Recovery Exercise/Contingency Plan Test, including coverage of external vendors' systems.
- AmeriCorps has not implemented the oversight necessary to conduct a thorough review and update all of its application's BIA to determine the prioritization, time, and recovery point objective for the application if interrupted or unavailable.
- AmeriCorps did not understand its role and responsibility to perform recovery activities for external vendors, including the ARC Financial System. In addition, AmeriCorps is placing reliance on external vendor systems and its requirement for BIA compliance for systems operated by shared service providers with the AmeriCorps environment. AmeriCorps lacks

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

clarity about responsibilities between the Agency and vendors for conducting business impact analysis and contingency plan development and testing. AmeriCorps claimed that ARC Financial System was incorporated with another application's BIA and was identified as a database. However, the database referred to in the application BIA and SSP was the database supporting the application. ARC, the shared service provider, used a different database.

The *AmeriCorps Managed Information Technology Services Disaster Recovery Plan* states that AmeriCorps must conduct annual disaster recovery testing that combines staff training. Training involves AmeriCorps staff and contractors participating in recovery exercises and certification based on the disaster recovery plan and certification worksheet. Annual testing/training aims to ensure that AmeriCorps personnel are prepared for disasters, familiar with procedures, and gain practical experience in recovery efforts. Additionally, the NIST Standard[10] requires organizations to test their contingency plans for federal information systems. The organizations determine the frequency and specific tests to assess plan effectiveness and readiness. Specifically, the *AmeriCorps Security Controls Catalog* requires the regular testing of the contingency plan for a system, at least annually. The testing can involve various methods, such as functional exercises, walk-throughs, tabletop exercises, checklists, and simulations.

NIST SP 800-53, Revision 5, *Security and Privacy Controls for Federal Information Systems and Organizations,* requires that organizations develop a Contingency Plan for each information system, in which the BIA's results are incorporated. 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. In addition, NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, outlines the three steps in establishing BIA and emphasizes the importance of maintaining an up-to-date Information System Contingency Plan (ISCP). The steps include determining mission/business processes and their criticality, identifying the resource requirements for recovery efforts, and establishing recovery priorities for system resources. NIST SP 800-34, Revision 1 also highlights the need for regular review and updates of the ISCP to ensure accuracy and completeness, particularly in response to significant changes in the ISCP, system, supported processes, or recovery resources. Further, *AmeriCorps Security Controls Family Catalog*, CP-2 Contingency Planning, requires the development of a Contingency Plan for each information system, including BIA results of identifying essential mission and business functions, 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 promptly continue operations of all necessary systems and functions. The GSS, eSPAN, an application, and ARC are environments that are constantly evolving and adapting to new or updated software and hardware.

[10] NIST SP 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, Page 119.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

This dynamic and consistently changing nature is driven by changes to operating systems, applications, and other components and by regular updates of patches and configurations to address bugs, security vulnerabilities, and performance improvements, as well as introducing new hardware devices into the network.

If a cybersecurity incident that limited access to ARC 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 prioritize recovery operations during a service-impacting incident effectively.

For an application, an inaccurate BIA can significantly hinder AmeriCorps' ability to respond to and recover from disruptions. It may lead to improper 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.

We recommend the AmeriCorps Chief Information Security Officer:

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. (**New**)
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. (**New**)
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. (**New**)
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. (**New**)
15) Develop a contingency plan and perform Business Impact Analysis for Administrative Resource Center Financial System. (**New**)

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Appendix I – Background

AmeriCorps[11] 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 eight information systems – the Network or GSS, eSPAN (which includes the eGrants grants management system), an application, 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 were rated as low security.[12] 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, one Field Financial Management Center, 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' Office of Information Technology (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 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. 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, incorporating NIST SP 800-53, Revision 5.

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

[12] 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.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Appendix II – Objective, Scope, and Methodology

Objective

The objective of our evaluation 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 evaluation in accordance with the *Quality Standards for Inspection and Evaluation,* issued by the Council of the Inspectors General on Integrity and Efficiency.[13] 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 assessment of relevant information security program and practices to report on the effectiveness of AmeriCorps' Agency-wide information security program for the period of October 1, 2022, through July 31, 2023, in accordance with the OMB's annual FISMA reporting instructions. We evaluated 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 5 for the following information systems:

- GSS;
- eSPAN;
- ARC; and
- an application.

The evaluation was conducted remotely due to the restrictions caused by the COVID-19 pandemic from October 1, 2022, through July 31, 2023. A network vulnerability assessment was also conducted at HQ.

In addition, the evaluation included an assessment of effectiveness for each of the nine[14] FY 2023 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.

[13] https://www.ignet.gov/sites/default/files/files/QualityStandardsforInspectionandEvaluation-2020.pdf
[14] Ibid, Page 5.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

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 2023 IG FISMA Metrics Domains aligned with the Cybersecurity Framework Security Functions. To accomplish the evaluation 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, IRP, 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 2022 FISMA report, including supporting documentation, to ascertain whether the actions taken addressed the weakness.[15] Refer to **Appendix III – Status of Prior Year Recommendations** 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-23-03, *Fiscal Year 2023 Guidance on Federal Information Security and Privacy Management Requirements*.
- FY 2023 IG FISMA Reporting Metrics.
- NIST SP 800-53, Revision 5, *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 5, *Assessing Security and Privacy Controls in 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 evaluation). In some cases, this resulted in selecting the entire population. However,

[15] *Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service*, OIG Report Number OIG-EV-22-03 (December 15, 2021).

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

in cases where the entire evaluation population was not selected, the results cannot be projected and, if projected, may be misleading.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Appendix III – Status of Prior Year Recommendations

During FY 2023, AmeriCorps implemented corrective actions to close 19 prior years' recommendations from the FY 2017 to FY 2022 FISMA evaluations. The remaining 14 recommendations are open, as depicted in **Table 5: Status of Prior Years' Recommendations**, and there are 15 new FY 2023 recommendations, as mentioned above in this report.

Table 5: Status of Prior Years' Recommendations

Evaluation	Auditor Position on Status of Recommendations[16]
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.	Open RMA determined this recommendation remains Open because the recommendation was not fully implemented. AmeriCorps developed policies to manage mobile devices and implemented mobile device protection measures for all devices except for the NCCC devices.
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.	Open RMA determined this recommendation remains Open because the recommendation was not fully implemented. AmeriCorps developed policies to manage mobile devices and implemented mobile device protection measures for all devices except for the NCCC devices.

[16] Status as of June 9, 2022.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation	Auditor Position on Status of Recommendations[16]
Recommendation 27: Ensure the facilities implement the following in regard to the protection of mobile devices: • 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. • Prohibit the use of non-governmental AmeriCorps issued email accounts.	Closed RMA testing showed the recommendation was implemented.
FY 2019	
Recommendation 1: Ensure that OIT monitors and promptly install patches and antivirus updates across the enterprise when they are available from the vendor. Enhancements should include: • Implement a process to track 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 showed the recommendation remained open. See Finding #2: 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 stated they were in progress in closing the recommendation. Expected completion date: March 30, 2024.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation	Auditor Position on Status of Recommendations[16]
Recommendation 4: Develop and implement a written process to ensure manual updates to the CMDB inventory and FasseTrack system are made simultaneously when the inventory is updated.	Open AmeriCorps stated they were in progress in closing the recommendation. Expected completion date: April 29, 2024.
Recommendation 5: Develop and implement a written process to ensure RemedyForce tickets are completed at the time the inventory is updated.	Closed RMA testing showed the recommendation was implemented.
Recommendation 6: Develop and implement a written process to perform periodic reconciliations between CMDB and the FasseTrack system.	Open AmeriCorps stated they were in progress in closing the recommendation. Expected completion date: April 29, 2024.
Recommendation 7: Perform and document analysis to determine the feasibility of completely automating the inventory management process.	Open AmeriCorps stated they were in progress in closing the recommendation. Expected completion date: April 29, 2024.
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 RMA testing showed the recommendation was implemented.
Recommendation 11: Implement Personal Identification Verification multifactor authentication for local and network access for privileged users to all workstations and servers.	Closed RMA testing showed the recommendation was implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation	Auditor Position on Status of Recommendations[16]
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 log-on with a Personal Identification Verification card.	Closed RMA testing showed the recommendation was implemented.
Recommendation 23: Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Open AmeriCorps stated they were in progress in closing the recommendation. Expected completion date: August 23, 2024.
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 AmeriCorps stated they were in progress in closing the recommendation. Expected completion date: August 23, 2024.
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 RMA testing showed the recommendation was implemented.
Recommendation 30: Develop and implement a written process to review and analyze the wireless network logs at the NCCC Pacific and Southwest Regional Campuses.	Closed RMA testing showed the recommendation was implemented.
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 RMA testing showed the recommendation was implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation	Auditor Position on Status of Recommendations[16]
FY 2020	
Recommendation 2: Specify how quickly users must apply security and operating system updates on CNCS mobile devices and implement a process to deny access to CNCS enterprise services for mobile devices that have not been updated within the prescribed period.	Closed RMA testing showed the recommendation was implemented.
Recommendation 3: Develop and implement a process to block unauthorized applications from installing on CNCS mobile devices.	Closed RMA testing showed the recommendation was implemented.
Recommendation 4: Complete the process of configuring the scanning tool to account for the approved deviations for the standard baseline configurations.	Open AmeriCorps considered this recommendation as completed; however, RMA determined this recommendation remains Open because the recommendation was not fully implemented. Although AmeriCorps established the policy, the baseline implementation is still in progress.
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 enormous number of personnel teleworking during the pandemic.	Closed RMA testing showed the recommendation was implemented.
Recommendation 9: Ensure all personnel whose responsibilities include access to PII complete annual privacy-role-based training.	Open AmeriCorps considered this recommendation as completed; however, RMA determined this recommendation remains Open because the recommendation was not fully implemented. Artifacts provided only address one specific person. All personnel who implement the privacy program whether technical or non-technical will also need to take the privacy-role-based training.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation	Auditor Position on Status of Recommendations[16]
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.	Open AmeriCorps provided supporting artifacts to close this recommendation on July 28, 2023; however, it was too late for RMA to test for the operational effectiveness before the issuance of this report.
Recommendation 2: Complete asset tracking refresher training for the Tier 2 support team.	Closed RMA testing showed the recommendation was implemented.
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.	Closed RMA testing showed the recommendation was implemented.
Recommendation 5: Document and implement an annual review process to validate that all agreements for system interconnections are kept current.	Closed RMA testing showed 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 progress in closing the recommendation. Expected completion date: September 30, 2023.
Recommendation 8: Immediately reinstate mandatory enforcement of multifactor authentication in accordance with CISA's recommendation.	Closed RMA testing showed the recommendation was implemented.
Recommendation 9: Update AmeriCorps' policy to require mandatory enforcement of multifactor authentication in the future, including in any hybrid work environment.	Closed RMA testing showed the recommendation was implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Evaluation	Auditor Position on Status of Recommendations[16]
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	Closed RMA testing showed the recommendation was implemented.
FY 2022	
Recommendation 1: 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.	Open AmeriCorps stated they were in progress in closing the recommendation. Expected completion date: March 15, 2024.
Recommendation 2: AmeriCorps perform an annual security and risk assessment for the application per AmeriCorps' policies.	Closed RMA testing showed the recommendation was implemented.
Recommendation 3: AmeriCorps implement the necessary oversight to monitor the continuity of operations plan (COOP) review process to ensure the plan is updated annually.	Closed RMA testing showed the recommendation was implemented.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

Appendix IV– Management's Comments

AmeriCorps

September 8, 2023

TO: Monique Colter, Assistant Inspector General for Audits

PRABHJOT BAJWA Digitally signed by PRABHJOT BAJWA Date: 2023.09.08 14:13:24 -04'00'

FROM: Prabhjot Bajwa, Chief Information Officer

SUBJECT: AmeriCorps management response to Report Number: OIG-EV-23-08 Request for Comments on the Office of Inspector General Draft Report on the Fiscal Year 2023 Federal Information Security Modernization Act Evaluation of AmeriCorps

This memorandum responds to the OIG-EV-23-08 request for comments on the Office of Inspector General draft report on the fiscal Year 2023 Federal Information Security Modernization Act Evaluation of AmeriCorps, issued August 24, 2023.

An integral part of AmeriCorps' ability to consistently implement and move towards an effective cybersecurity program has been through the implementation of corrective action plans and improvements based on the findings and recommendations provided by the OIG through its annual Federal Information Security Modernization Act Evaluation audit. We continue to value these engagements and believe in the integrity and importance of audit process.

AmeriCorps' leadership continues to agree with all the findings made by the OIG. We appreciate the time, communication, and collaboration that went into this year's audit. We value the OIG's actionable steps and risk-based approach documented in the recommendations, particularly around identifying areas of opportunities to improve the effectiveness of its cybersecurity program. AmeriCorps remains committed to remediating cybersecurity risks, continuing to work diligently to strengthen the maturity of its enterprise-wide cybersecurity program, and elevate cybersecurity maturity across all Federal Information Security Modernization Act Evaluation domains. Based on the prioritization and commitment to improving cybersecurity maturity, significant changes were made during FY 2023:

- Implementation of corrective actions associated to the "Identify" security function showing measurable improvement.
- Implementation of organization-wide Personal Identification Verification multifactor authentication for privileged and non-privileged users.
- Implementation of corrective actions associated to the "Protect" security function showing measurable improvement.
- Implementation of mobile device protection measures:
    - Processes to block installation of unauthorized applications.
    - Processes to enforce the installation of security and operating system updates within organization defined timeframes.
    - Processes to enforce password requirements.

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

- Processes to prohibit the use of non-governmental AmeriCorps issued email accounts.
- Implementation of processes to reimage information technology assets upon separation.

- Consistently reporting incidents to United States Computer Emergency Readiness Team within required timeframes.

AmeriCorps remains committed to improving its cybersecurity program by developing actionable project plans and corrective action plans to develop, implement, and manage the following areas of opportunity:

- Develop an AmeriCorps Common Control Provider system that will serve as the overarching System Security Plan documenting the following:
  - AmeriCorps' information system inventory of all information systems
  - Technical description documenting the technical landscape of AmeriCorps system interconnections and including third-party providers, cloud service providers, etc.
  - Security control implementation approaches to identify inheritable AmeriCorps controls (i.e. policy, program management, personally identifiable information processing and transparency, supply chain risk management, and organization-defined parameters for hybrid controls.
- Continue working with information system owners to ensure Incident and Breach Response Training and Tabletop exercises are conducted annually, including contingency planning and disaster recovery efforts.
- Improve vulnerability and patch management processes by ensuring industry standards and best practices identified by the Cybersecurity and Infrastructure Security Agency and National Institute of Standards and Technology are accounted for and included in updated vulnerability and patch management procedures.
- Develop schedules to ensure cybersecurity policies are reviewed and updated in accordance with AmeriCorps defined frequencies.
- Develop schedules to ensure information systems and authorization packages are completed and signed in accordance with AmeriCorps defined frequencies.
- Assess current security posture by conducting document reviews, risk assessments, vulnerability scans, and internal assessments to measure our performance against industry standards and best practices to identify strengths and weaknesses of existing security policies, procedures, controls, and measures to include the review of unsupported software.
- Implement 'security-by-design' integrating appropriate security measures, mechanisms, and techniques into every stage of the System Development Lifecycle, to include Business Impact Analysis updates and implementation of event logging capabilities.

We appreciate the opportunity to provide input on the OIG's report. If you have any questions, please feel free to contact me directly at **pbajwa@cns.gov** or (202) 391-4072. Or,

1005 N. Glebe Road, Suite 610
Arlington, VA 22201
Phone: (571) 429-6600
www.rmafed.com

your team can contact Bilal Razzaq, chief information security officer, at **brazzaq@cns.gov** or (202) 693-1567.

CC:

Stephen Ravas, Acting Inspector General
Kim Benoit, Acting Deputy Inspector General
Monique Colter, Assistant Inspector General for Audit
George Fallon, Principal, RMA Associates, LLC
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
Fernando Laguarda, General Counsel
Malena Brookshire, Chief Financial Officer
Rachel Turner, Audits & Investigations Program Manager

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