AmeriCorps
Office of Inspector General

FY 2025 Federal Information Security Modernization Act (FISMA) Audit

Audit Report

OIG-AR-25-03

February 2, 2026

AmeriCorps
Office of Inspector General

February 2, 2026

MEMORANDUM TO: Bilal Razzaq
Chief Information Security Officer

FROM: Lauren Lesko LAUREN LESKO Digitally signed by LAUREN LESKO Date: 2026.02.02 11:19:58 -05'00'
Assistant Inspector General for Audits

SUBJECT: Fiscal Year 2025 Federal Information Security Modernization Act Audit (Report Number: OIG-AR-25-03)

Enclosed is the AmeriCorps Office of Inspector General's (OIG) final report on the Fiscal Year (FY) 2025 Federal Information Security Modernization Act (FISMA) Audit (Report Number: OIG-AR-25-03).

AmeriCorps OIG contracted with the independent certified public accounting firm Sikich, LLC (Sikich) to conduct the FY 2025 FISMA audit. Sikich is responsible for the attached final report. We reviewed Sikich'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 Sikich 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 final report, please contact me at (202) 880-9292 or l.lesko@americorpsoig.gov.

cc: Jennifer Bastress Tahmasebi, Interim Agency Head
Charndrea Leonard, Acting Chief Operating Officer
Sandra Washington, Acting Chief Information Officer
Sarah Mirzakhani, Principal, Sikich, LLC
Jeff Davis, Principal, Sikich, LLC

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.

SIKICH®

TABLE OF CONTENTS

I. EXECUTIVE SUMMARY 1

INTRODUCTION 1
SUMMARY OF AUDIT RESULTS 2
SUMMARY OF AMERICORPS MANAGEMENT'S RESPONSE 4
AUDITOR'S EVALUATION OF AMERICORPS MANAGEMENT'S RESPONSE 4

II. FISMA AUDIT FINDINGS 6

FUNCTION: GOVERN 6
Finding 1: AmeriCorps Did Not Develop an Organizational Cybersecurity Profile or Related Policies and Procedures. 6
FUNCTION: IDENTIFY 7
Finding 2: AmeriCorps Did Not Complete an Inventory of Its Data and Corresponding Metadata. 7
FUNCTION: PROTECT 9
Finding 3: AmeriCorps' Servers, Workstations, and Network Devices Did Not Fully Comply with Established Standard Baseline Configurations. 9
Finding 4: AmeriCorps Did Not Consistently Resolve Vulnerabilities for Servers and Workstations Within the Required Timelines. 10
FUNCTION: DETECT 11
Finding 5: AmeriCorps Did Not Consistently Complete Annual Security Control Assessments and System Risk Assessments. 11
FUNCTION: RECOVER 13
Finding 6: The Recovery Time Objective (RTO) for the eSPAN System Is Not Aligned with the GSS RTO. 13

APPENDIX A: BACKGROUND 15

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY 17

APPENDIX C: STATUS OF PRIOR-YEAR RECOMMENDATIONS 20

APPENDIX D: MANAGEMENT COMMENTS 23

APPENDIX E: ACRONYM LIST 25

SIKICH®

I. EXECUTIVE SUMMARY

INTRODUCTION

The Federal Information Security Modernization Act of 2014 (FISMA) requires federal agencies to develop, document, and implement an agency-wide information security program to protect their information and information systems, including those provided or managed by another agency, contractor, or other source. Agencies must also conduct an annual independent audit of their information security program and practices to be performed by the Inspector General or an independent external auditor and report results to the Office of Management and Budget (OMB) and to Congressional committees.

AmeriCorps' Office of the Inspector General (OIG) engaged Sikich CPA LLC (Sikich)[1] to conduct the FISMA audit for Fiscal Year (FY) 2025. The objective of this audit was to assess the effectiveness of AmeriCorps' information security program and practices for the period October 1, 2024, through July 31, 2025, in accordance with FISMA.

The audit included the testing of select controls outlined in National Institute of Standards and Technology (NIST) guidance[2] for the following sample of 4 of the 23 information systems[3] in AmeriCorps' system inventory as of March 17, 2025:

- 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.

The FY 2025 Inspector General (IG) FISMA Reporting Metrics required IGs to assess 20 core[4] and five supplemental[5] IG FISMA Reporting Metrics across six function areas—Govern, Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of the agency's information security program and the maturity level of each function area, as highlighted in **Table 1**.

[1] Effective August 30, 2024, Sikich CPA LLC acquired assets—including federal contracts subject to novation—from Saggar & Rosenberg, P.C. (S&R). As part of closing on the transaction, S&R entered into an overall subcontract agreement with Sikich for the execution of the aforementioned contracts, including those with AmeriCorps. S&R and Sikich have submitted a novation package to the Government, consistent with 48 Code of Federal Regulations (C.F.R.) § 42.1204.

[2] NIST Special Publication (SP) 800-53, Revision 5, *Security and Privacy Controls for Information Systems and Organizations*, supporting the *FY 2025 Inspector General Federal Information Security Modernization Act of 2014 (FISMA) Reporting Metrics v2.0* (FY 2025 IG FISMA Reporting Metrics).

[3] According to the NIST Glossary, an information system is a discrete set of information resources organized for the collection, processing, maintenance, use, sharing, dissemination, or disposition of information.

[4] Core metrics are assessed annually and represent a combination of administration priorities, high-impact security processes, and essential functions necessary to determine the effectiveness of a security program. The core metrics can be found in the FY 2025 IG FISMA Reporting Metrics online here.

[5] Supplemental metrics are assessed at least once every two years; they represent important activities conducted by security programs and contribute to the overall evaluation and determination of the effectiveness of the security program. The supplemental metrics can be found in the FY 2025 IG FISMA Reporting Metrics online here.

Table 1: Alignment of the NIST Cybersecurity Framework (CSF) Functions to the Domains in the FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions	Function Area Objective	Domain(s)
Govern	The organization's cybersecurity risk management strategy, expectations, and policy are established, communicated, and monitored.	Cybersecurity Governance and Cybersecurity Supply Chain Risk Management
Identify	The organization's current cybersecurity risks are understood.	Risk and Asset Management
Protect	Safeguards to manage the organization's cybersecurity risks are used.	Configuration Management, Identity and Access Management, Data Protection and Privacy, and Security Training
Detect	Possible cybersecurity attacks and compromises are found and analyzed.	Information Security Continuous Monitoring
Respond	Actions regarding a detected cybersecurity incident are taken.	Incident Response
Recover	Assets and operations affected by a cybersecurity incident are restored.	Contingency Planning

Source: Sikich's analysis of NIST CSF 2.0 and the FY 2025 IG FISMA Reporting Metrics

The foundational (lower) levels of the maturity model in the IG FISMA Reporting Metrics focus on the development of sound, risk-based policies and procedures, while the advanced (higher) levels capture the institutionalization and effectiveness of those policies and procedures. **Table 2** below explains the five maturity model levels. A functional information security area is not considered effective unless it achieves a rating of at least Level 4: *Managed and Measurable.*

Table 2: IG Evaluation Maturity Levels

Maturity Level	Maturity Level Description
Level 1: Ad-hoc	Policies, procedures, and strategies are not formalized; activities are performed in an ad-hoc, reactive manner.
Level 2: Defined	Policies, procedures, and strategies are formalized and documented but not consistently implemented.
Level 3: Consistently Implemented	Policies, procedures, and strategies are consistently implemented, but quantitative and qualitative effectiveness measures are lacking.
Level 4: Managed and Measurable	Quantitative and qualitative measures on the effectiveness of policies, procedures, and strategies are collected across the organization and used to assess the policies and procedures and make necessary changes.
Level 5: Optimized	Policies, procedures, and strategies are fully institutionalized, repeatable, self-generating, consistently implemented, and regularly updated based on a changing threat and technology landscape and business/mission needs.

Source: FY 2025 IG FISMA Reporting Metrics

SUMMARY OF AUDIT RESULTS

We concluded that AmeriCorps did not implement an effective information security program because its security program was not consistent with FISMA requirements, OMB policy and guidance, or NIST standards and guidelines and it fell short of the overall maturity rating of Level 4: *Managed and Measurable*. AmeriCorps' information security program achieved an overall rating of Level 3: *Consistently Implemented*. Below, **Table 3** summarizes AmeriCorps' overall maturity levels for each CSF function and domain in the FY 2025 IG FISMA Reporting Metrics. We determined that one CSF function achieved a Level 4: *Managed and Measurable* maturity level, three CSF functions achieved a Level 3: *Consistently Implemented* maturity level, and two achieved a Level 2: *Defined* maturity level.

Table 3: AmeriCorps' Maturity Levels for FY 2025 IG FISMA Reporting Metrics

Cybersecurity Framework Functions	Maturity Level by Function	Domain	Maturity Level by Domain
Govern	Level 2: *Defined*	Cybersecurity Governance	Level 2: *Defined*
		Cybersecurity Supply Chain Risk Management	Level 2: *Defined*
Identify	Level 2: *Defined*	Risk and Asset Management	Level 2: *Defined*
Protect	Level 3: *Consistently Implemented*	Configuration Management	Level 2: *Defined*
		Identity and Access Management	Level 4: *Managed and Measurable*
		Data Protection and Privacy	Level 3: *Consistently Implemented*
		Security Training	Level 4: *Managed and Measurable*
Detect	Level 3: *Consistently Implemented*	Information Security Continuous Monitoring	Level 3: *Consistently Implemented*
Respond	Level 4: *Managed and Measurable*	Incident Response	Level 4: *Managed and Measurable*
Recover	Level 3: *Consistently Implemented*	Contingency Planning	Level 3: *Consistently Implemented*
Overall	**Level 3: *Consistently Implemented* (Not Effective)**		

Source: Sikich's assessment of AmeriCorps' information security program controls and practices based on the FY 2025 IG FISMA Reporting Metrics.

We found that AmeriCorps established several information security program controls and practices that were consistent with FISMA requirements, OMB policy and guidelines, and applicable NIST standards and guidelines. For example, AmeriCorps:

- Integrated cybersecurity risk management information into Enterprise Risk Management (ERM) reporting tools.
- Consistently implemented strong authentication mechanisms for both privileged and non-privileged users to authenticate to applicable organizational systems.
- Employed automation to track the life cycle of the organization's software assets and their associated licenses.
- Implemented advanced logging requirements at the Event Logging (EL) 1 maturity level (basic), EL2 maturity level (intermediate), and EL3 maturity level (advanced) in accordance with OMB requirements.[6]

Furthermore, AmeriCorps made progress in implementing prior-year recommendations. During FY 2025, AmeriCorps closed 10 of the 15 open recommendations from prior years,[7] thus maintaining a consistently implemented information security program. However, AmeriCorps must make further improvements in its information security for the program to be effective.

[6] OMB Memorandum M-21-31, *Improving the Federal Government's Investigative and Remediation Capabilities Related to Cybersecurity Incidents* (August 27, 2021), establishes a maturity model to guide the implementation of requirements across four EL tiers.
[7] See Appendix C for the status of prior-year recommendations.

In addition, this report describes security control weaknesses that reduced the effectiveness of AmeriCorps' information security program and practices. Specifically, we identified deficiencies across several domains of the FY 2025 IG FISMA Reporting Metrics, including Cybersecurity Governance, Risk and Asset Management, Configuration Management, Information Security Continuous Monitoring, and Contingency Planning. These control weaknesses impacted AmeriCorps' maturity levels across the function areas, as shown in **Table 4**.

Table 4: Control Weaknesses by Function and Domain

Function	Domain	Control Weakness
Govern	Cybersecurity Governance	AmeriCorps did not develop an organizational cybersecurity profile or related policies and procedures **(Finding 1)**.
Identify	Risk and Asset Management	AmeriCorps did not complete an inventory of its data and corresponding metadata **(Finding 2)**.
Protect	Configuration Management	AmeriCorps' servers, workstations, and network devices did not fully comply with established standard baseline configurations (**Finding 3**). AmeriCorps did not consistently resolve vulnerabilities for servers and workstations within the required timelines (**Finding 4**).
Detect	Information Security Continuous Monitoring	AmeriCorps did not consistently complete annual Security Control Assessments (SCAs) and system risk assessments **(Finding 5)**.
Recover	Contingency Planning	The Recovery Time Objective (RTO) for the Electronic System for Programs, Agreements and National Service Participants (eSPAN) system is not aligned with the General Support System (GSS) RTO **(Finding 6)**.

To help strengthen AmeriCorps' information security program and practices, we have issued nine new recommendations. Additionally, five prior-year recommendations remain open.[8]

SUMMARY OF AMERICORPS MANAGEMENT'S RESPONSE

AmeriCorps remains committed to addressing cybersecurity risks, diligently working to strengthen the maturity of the agency's enterprise-wide cybersecurity program, and elevating cybersecurity maturity across all Cybersecurity Framework domains. AmeriCorps provided comments on the draft FY 2025 FISMA audit report, conducted by Sikich CPA LLC, and concurred with the audit findings. AmeriCorps' comments are included in their entirety in **Appendix D**.

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 2025 FISMA audit. We acknowledge that AmeriCorps concurred with the audit findings, and their stated commitment to address cybersecurity risks and strengthen the maturity of the agency's enterprise-wide cybersecurity program.

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

[8] See Appendix C for the status of prior-year recommendations.

The following section provides a detailed discussion of the findings by NIST CSF function area and domain. **Appendix A** provides background information on AmeriCorps and relevant criteria. **Appendix B** describes the audit objective, scope, and methodology. **Appendix C** summarizes the status of recommendations made in prior-year FISMA reports. **Appendix D** includes management's comments, and **Appendix E** defines the acronyms used within this report.

Sikich CPA LLC

Alexandria, VA
January 30, 2026

SIKICH®

II. FISMA AUDIT FINDINGS

FUNCTION: GOVERN

FY 2025 IG FISMA Reporting Metrics Domain: Cybersecurity Governance

Finding 1: AmeriCorps Did Not Develop an Organizational Cybersecurity Profile or Related Policies and Procedures.

Executive Order 13800, *Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure* (May 11, 2017), states:

> *Each agency head shall use The Framework for Improving Critical Infrastructure Cybersecurity (the Framework)*[9] *developed by NIST, or any successor document, to manage the agency's cybersecurity risk.*

The Government Accountability Office's (GAO's) *Standards for Internal Control in the Federal Government* (September 2014), GAO-14-704G, *Principle 12 – Implement Control Activities*, states:

> *12.01 – Management should implement control activities through policies.*

We inquired with AmeriCorps management about the extent to which the agency develops and maintains cybersecurity profiles[10] to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives. AmeriCorps management indicated that its established cybersecurity practices inherently address the core components of cybersecurity profiles in alignment with NIST CSF 2.0.[11]

However, based on our review of AmeriCorps' cybersecurity program documentation, we found that, while the documentation reflects AmeriCorps' implementation of its cybersecurity program, AmeriCorps has not developed or maintained an organizational cybersecurity profile to understand, tailor, assess, prioritize, and communicate its cybersecurity objectives in accordance with NIST CSF 2.0. In addition, AmeriCorps has not documented its policies, procedures, or guidance for performing NIST CSF 2.0 activities to facilitate the development and maintenance of an organizational cybersecurity profile, including analyses to account for changes in its cybersecurity posture.

AmeriCorps management stated that, while the organization does not maintain standalone documents explicitly titled "Current Cybersecurity Profile" and "Target Cybersecurity Profile" aligned with NIST CSF 2.0 terminology, it believes its established cybersecurity practices inherently address the core components of this concept. AmeriCorps stated that it uses documented baseline security controls, results of recent assessments and audits, a gap

[9] Before version 2.0, CSF was called the "Framework for Improving Critical Infrastructure Cybersecurity." This title is not used for NIST CSF 2.0.
[10] NIST CSF 2.0 (February 26, 2024) provides guidance to assist with managing cybersecurity risks. Section 3.1 offers guidance on the use of cybersecurity profiles to understand, tailor, assess, prioritize, and communicate cybersecurity objectives. A CSF organizational profile describes an organization's current and/or target cybersecurity posture in terms of the CSF core's outcomes. The CSF core is a taxonomy of high-level cybersecurity outcomes that can help organizations manage their cybersecurity risks. The CSF core components are a hierarchy of functions, categories, and subcategories that detail each outcome.
[11] See the NIST CSF 2.0 online here.

analysis displaying an enterprise-wide view of cybersecurity risks, and a risk register to understand, tailor, assess, prioritize, and communicate AmeriCorps' cybersecurity objectives.

In addition, AmeriCorps stated that the *Roadmap of AmeriCorps Cybersecurity Program Plan* and *Enterprise Risk Management Program* policy—along with other policies, standards, and procedures—comprehensively address the underlying sentiment of the requirements of an organizational cybersecurity profile.

However, our review determined that although these documents demonstrate AmeriCorps' implementation of its cybersecurity program, they fall short of the objective of the NIST CSF organizational cybersecurity profile with regard to identifying the current status of the CSF functional outcomes and the target priority to enable AmeriCorps to identify and analyze the differences between the current and target cybersecurity posture profiles.

AmeriCorps management also stated they are actively engaged in a continuous improvement process and are committed to full implementation of NIST CSF 2.0. This includes formalizing documentation practices to align precisely with NIST CSF 2.0 terminology and structure in the future.

Without documenting current and target CSF organizational profiles—including a gap analysis between the current and target cybersecurity posture—there is increased risk that AmeriCorps has not appropriately planned for or addressed relevant cybersecurity risks/issues, including—but not limited to—breaches, system interruptions, and vulnerability exploitation.

To assist AmeriCorps with implementing the NIST CSF profiles, we recommend that AmeriCorps' Chief Information Security Officer (CISO):

Recommendation 1: Review NIST CSF 2.0 and formalize documented policies and procedures for developing and maintaining current and target cybersecurity profiles that align with the CSF to include, at a minimum, consideration of AmeriCorps' mission objectives, threat landscape, and resources (including personnel) and constraints.

Recommendation 2: Develop, document, and maintain current and target cybersecurity profiles that align with NIST CSF 2.0—including a gap analysis between the current and target cybersecurity postures—and that consider anticipated changes in AmeriCorps' cybersecurity posture.

FUNCTION: IDENTIFY

FY 2025 IG FISMA Reporting Metrics Domain: Risk and Asset Management

Finding 2: AmeriCorps Did Not Complete an Inventory of Its Data and Corresponding Metadata.

Public Law (Pub. L.) No. 115-435, *Foundations for Evidence-Based Policymaking Act of 2018*, Title II – Open Government Data Act, requires the head of each agency, to the maximum extent practicable, to develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency. The inventory is to provide a clear and comprehensive understanding of the data assets in the possession of the agency.

In addition, OMB issued guidance in Memorandum M-25-05, *Phase 2 Implementation of the Foundations for Evidence-Based Policymaking Act of 2018: Open Government Data Access and Management Guidance*, which states:

> *4. Agency Requirements that Apply to All Data Assets*
>
> *a. Comprehensive Data Inventories*
>
> *Agencies must, to the maximum extent practicable, develop and maintain a comprehensive data inventory that accounts for all data assets created by, collected by, under the control or direction of, or maintained by the agency (hereinafter "in the possession of the agency"), with the exception of data assets contained on a national security system.*

Based on a walkthrough of AmeriCorps' data inventory project in the Microsoft Purview data governance tool, we found that AmeriCorps has not fully completed a comprehensive and accurate inventory of data and corresponding metadata for its data types, to include data obtained from third-party providers. In addition, AmeriCorps has not specifically documented policies and procedures for developing and maintaining a data and metadata inventory for its data types.

AmeriCorps management stated that Microsoft Purview is in the process of being implemented as the agency's unified data governance solution for completing a comprehensive and accurate inventory of data and corresponding metadata for its data types, to include data obtained from third-party providers. However, AmeriCorps stated that Microsoft Purview is not yet ready for implementation of retention labels, policies, and information sensitivity labels. AmeriCorps stated its recent work toward automation and optimization includes creation of a Microsoft Purview file plan. AmeriCorps management further stated that this file plan, which includes National Archives and Records Administration and agency-specific schedules, is approximately 90 percent complete and still requires editing and creation of related logging and tracking of various Purview activities and actions.

Without maintaining a comprehensive and accurate inventory of AmeriCorps' data and corresponding metadata, there is an increased risk that AmeriCorps may not properly account for and secure sensitive data.

To assist AmeriCorps with maintaining the inventory of data and corresponding metadata, we recommend that AmeriCorps' Chief Data Officer:

Recommendation 3: Document policies and procedures for developing and maintaining a comprehensive and accurate inventory of data and the corresponding metadata for AmeriCorps' data types.

Recommendation 4: Develop and maintain a comprehensive and accurate inventory of data and corresponding metadata for AmeriCorps' data types, to include data obtained from third-party providers, to meet the requirements of the Open Government Data Act and OMB Memorandum M-25-05.

FUNCTION: PROTECT

FY 2025 IG FISMA Reporting Metrics Domain: Configuration Management

Finding 3: AmeriCorps' Servers, Workstations, and Network Devices Did Not Fully Comply with Established Standard Baseline Configurations.

AmeriCorps' *Security Control Standard Configuration Management*, Version 1.1 (March 19, 2025), requires establishing and documenting configuration settings for components employed within the system that reflect the most restrictive mode consistent with operational requirements using organizational approved baseline configurations and implementing the configuration settings.

Based on inspection of AmeriCorps' baseline compliance reports, we found that AmeriCorps' operating systems and network devices were not fully compliant with the established standard baseline configurations. Specifically, we noted the following:

- 41 percent of standard baseline configuration settings failed compliance checks on Windows Server 2012.
- 48 percent of standard baseline configuration settings failed compliance checks on Windows Server 2016.
- 47 percent of standard baseline configuration settings failed compliance checks on Windows Server 2019.
- 18 percent of standard baseline configuration settings failed compliance checks on Windows Server 2022.
- 12 percent of standard baseline configuration settings failed compliance checks on Cisco switches and firewalls.
- 10 percent of standard baseline configuration settings failed compliance checks on Windows 10 and 11 workstations.

AmeriCorps management indicated that the Windows 2012 servers have reached end-of-life and are being decommissioned. Therefore, no further efforts will be made to ensure compliance with standard baseline configurations for these servers.

AmeriCorps management also indicated that baseline compliance scans for the remaining network servers, workstations, and network devices did not account for approved deviations and false positives. However, our review of the baseline configuration documents indicated that approved deviations are excluded from compliance scan reports. Furthermore, management did not provide additional evidence to support its statement regarding approved deviations and false positives.

Management attributed the lack of supporting documentation to significant staffing reductions that occurred in April 2025, which prevented management from providing documentation for auditor evaluation.

Without complying with baseline configurations, AmeriCorps risks having misconfigured and insecure systems on its network. Misconfigured and insecure systems make it difficult for AmeriCorps to ensure its information systems are adequately secured and protected and place the systems and the agency at risk for compromise.

To assist AmeriCorps with fully implementing standard baseline configurations, we recommend that the CISO:

Recommendation 5: Implement the approved standard baseline configurations for all servers, workstations, and network devices in AmeriCorps' information system environment.

Finding 4: AmeriCorps Did Not Consistently Resolve Vulnerabilities for Servers and Workstations Within the Required Timelines.

AmeriCorps' *Patch Management Process*, Version 4.0 (January 2025), states the following regarding patching timeframes for critical and high-severity vulnerabilities:

> *Critical (Very High) and High Severity: These patches address vulnerabilities that pose significant risks to system security, data integrity, and overall operations. Critical vulnerabilities may be actively exploited or have the potential for widespread impact, while high-severity vulnerabilities could significantly affect system performance or security. Patches for these vulnerabilities will be deployed within 30 days of initial detection. This rapid deployment ensures that AmeriCorps systems are protected from severe threats in a timely manner.*

In addition, the Cybersecurity and Infrastructure Security Agency's (CISA's)[12] Binding Operational Directive 22-01, *Reducing the Significant Risk of Known Exploited Vulnerabilities* (November 3, 2021), states that agencies are required to remediate each vulnerability according to the timelines set forth in the CISA-managed vulnerability catalog. The catalog lists exploited vulnerabilities that carry significant risk to the federal enterprise and requires agencies to remediate vulnerabilities within 6 months for vulnerabilities with a Common Vulnerabilities and Exposures (CVE)[13] identification number assigned prior to 2021 and within 2 weeks for all other vulnerabilities. These default timelines may be adjusted in the case of grave risk to the federal enterprise.

Using vulnerability data from the Common Vulnerability Scoring System (CVSS)[14] used by Nessus, we identified unpatched software, unsupported software, and improper configuration settings that exposed AmeriCorps' network to critical[15] and high-severity[16] vulnerabilities. Specifically, we identified 1 critical and 6 high-severity vulnerabilities present on AmeriCorps' servers and 40 critical and 348 high-severity vulnerabilities on AmeriCorps' workstations that were not remediated within 30 days of initial detection, as required by its internal operating policies.

[12] CISA, a component of the Department of Homeland Security, leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure.
[13] CVE is a list of all publicly known vulnerabilities that include the CVE identification number.
[14] CVSS provides a way to capture the principal characteristics of a vulnerability and produce a numerical score reflecting its severity. The numerical score can then be translated into a qualitative representation (such as low, medium, high, and critical) to help organizations properly assess and prioritize their vulnerability management processes. CVSS is a published standard used by organizations worldwide.
[15] The critical rating is based on CVSS version 3, which provides a standardized way of reporting vulnerabilities by the risk they pose to an organization. Critical vulnerabilities possess a rating of 9.0 to 10.0.
[16] High-risk vulnerabilities possess a CVSS rating of 7.0 to 8.9.

In addition, we identified 114 CISA Known Exploitable Vulnerabilities (KEVs) on the servers and 429 CISA KEVs on the workstations that were not remediated by the CISA-required remediation date.[17] Due dates for the KEVs ranged from December 2021 through May 2025.

AmeriCorps management stated that the one critical-severity vulnerability present on the servers was identified April 18, 2025, and patched by May 21, 2025, and the six high-severity vulnerabilities were remediated by May 22, 2025. AmeriCorps attributed the missed deadline to patch this critical vulnerability to an organization-wide Reduction in Force (RIF) effort beginning on April 16, 2025, that placed the dedicated team responsible for remediating vulnerabilities on administrative leave and further stated that once team members were reassigned to manage the process, vulnerability management activities were able to resume.

Management also stated that, of the 40 critical workstation vulnerabilities, 5 of the workstations belong to individuals who were also placed on administrative leave and have not connected to the network. The remaining 35 are pending a user-dependent browser self-update.

Management stated that, of the 348 high-severity workstation vulnerabilities, 252 are pending a user-dependent browser self-update and 43 are related to workstations that belong to employees who were also placed on administrative leave. The remaining 53 are a result of a product that is no longer supported.

In addition, management stated that the 114 CISA KEVs on the servers and 429 CISA KEVs on the workstations are related to the previously identified vulnerabilities.

Absent the timely installation of required patches, implementation of secure configuration settings, and migration to supported software, AmeriCorps cannot effectively mitigate security vulnerabilities or reduce the risk of compromise to the confidentiality, integrity, and availability of sensitive data.

A prior-year FISMA recommendation[18] regarding the tracking of patching for network devices and servers, the replacement of unsupported software, and the monitoring of vulnerability remediation remains open. Therefore, we are not making a new recommendation related to this finding.

FUNCTION: DETECT

FY 2025 IG FISMA Reporting Metrics Domain: Information Security Continuous Monitoring

Finding 5: AmeriCorps Did Not Consistently Complete Annual Security Control Assessments and System Risk Assessments.

AmeriCorps' *Cybersecurity Information Security Continuous Monitoring Policy*, Version 7 (February 9, 2025), requires annual risk assessment reviews and assessments of security controls in accordance with the AmeriCorps Security Assessment and Authorization standard operating procedures, to support ongoing authorization.

[17] To help organizations better manage vulnerabilities and keep pace with threat activity, CISA maintains the authoritative source of vulnerabilities that have been exploited in the wild, along with the date by which agencies are required to remediate each vulnerability. See CISA Known Exploited Vulnerabilities Catalog for more details.
[18] Recommendation 1, *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 20-03, January 24, 2020). Refer to Appendix C for additional information regarding the prior-year recommendations.

AmeriCorps' *Security Control Standard Assessment, Authorization & Monitoring*, Version 1.1 (February 21, 2025), control CA-02 - Control Assessments, requires critical and volatile controls to be self-assessed and independently evaluated annually. In addition, one-third of assigned controls will be self-assessed and independently evaluated annually to complete a full assessment every 3 years.

In addition, NIST SP 800-53, Revision 5, requires conducting risk assessments that include:

1. *Identifying threats to and vulnerabilities in the system;*
2. *Determining the likelihood and magnitude of harm from unauthorized access, use, disclosure, disruption, modification, or destruction of the system, the information it processes, stores, or transmits, and any related information; and*
3. *Determining the likelihood and impact of adverse effects on individuals arising from the processing of personally identifiable information.*

Furthermore, NIST SP 800-53, Revision 5, states the following regarding risk assessments for third-party systems:

> *Risk assessments also consider risk from external parties, including contractors who operate systems on behalf of the organization, individuals who access organizational systems, service providers, and outsourcing entities.*

We requested the most recent risk assessment for the Department of Treasury's Bureau of the Fiscal Service's ARC system, a third-party system used by AmeriCorps, and found that AmeriCorps did not document a risk assessment for the system.

Additionally, our review of the most recent annual SCA and risk assessment for the GSS and eSPAN found that AmeriCorps did not perform an annual SCA or update the risk assessments annually for the GSS and eSPAN. The most recent SCA and risk assessment updates for both systems were completed in 2023.

Regarding the ARC risk assessment, AmeriCorps management stated that they reviewed ARC's FISMA documentation and although they did not perform a separate, formal risk assessment for security controls, the ARC Business Impact Analysis (BIA) serves as AmeriCorps' internal risk assessment for the impact of service disruption.

Although a BIA addresses risks related to system disruptions, it does not include broader risk assessment requirements, such as security and privacy threats, identifying vulnerabilities associated with the use of the ARC system, assessing potential impacts from threat exploitation, or evaluating the likelihood and magnitude of harm for those vulnerabilities and threats.

Regarding the risk assessments for the GSS and eSPAN, AmeriCorps management stated that risks are formally documented through Security Impact Analyses (SIAs) conducted throughout the year for system changes and addressed through the continuous monitoring program. AmeriCorps also stated that the SIA process conducted for proposed system changes evaluates relevant controls and is reviewed by the Change Control Board, the Information System Security Officer, and the CISO.

However, while SIAs assess controls related to specific changes, they do not provide a comprehensive analysis of system-wide security and privacy threats, vulnerabilities, or the likelihood and impact of potential adverse effects.

Regarding the lack of SCAs for the GSS and eSPAN in 2024, AmeriCorps management stated that the agency was in process of redesigning its continuous monitoring plan when the resource responsible for these activities was no longer available.

Without conducting annual SCAs and maintaining up-to-date risk assessments, AmeriCorps does not have reasonable assurance that controls are operating effectively, which may expose AmeriCorps to information loss, fraud, or abuse. In addition, the lack of timely assessments and/or continuous monitoring limits authorizing officials' ability to make effective decisions regarding the risk for compromise created by system operations.

To assist AmeriCorps with consistently implementing their continuous monitoring processes, we recommend that AmeriCorps' CISO:

Recommendation 6: Perform and document a formal risk assessment associated with the use of the ARC system.

Recommendation 7: Update the risk assessments for the GSS and eSPAN on an annual basis.

Recommendation 8: Conduct an SCA for the GSS and eSPAN on an annual basis in accordance with AmeriCorps' *Security Control Standard Assessment, Authorization & Monitoring*.

FUNCTION: RECOVER

FY 2025 IG FISMA Reporting Metrics Domain: Contingency Planning

Finding 6: The Recovery Time Objective (RTO) for the eSPAN System Is Not Aligned with the GSS RTO.

AmeriCorps' *Security Control Standard Contingency Planning*, Version 1.2 (March 20, 2025), control CP-02(1), Contingency Plan | Coordinate with Related Plans, requires coordinating contingency plan development with organizational elements responsible for related plans.

In addition, NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems* (May 2010), section 3.2.1: Determine Business Processes and Recovery Criticality, states:

> *To accomplish the BIA and better understand the impacts a system outage or disruption can have on the organization, the Information System Contingency Plan (ISCP) Coordinator should work with management and internal and external points of contact to identify and validate mission/business processes and processes that depend on or support the information system.*
>
> *The ISCP Coordinator should next analyze the supported mission/business processes and with the process owners, leadership, and business managers determine the*

acceptable downtime if a given process or specific system data were disrupted or otherwise unavailable.

The eSPAN BIA identified a RTO[19] of 12 hours, while the GSS BIA identified the RTO as 96 hours for major applications, including eSPAN. Therefore, the RTO for the eSPAN application is not aligned with the GSS BIA that supports the application.

AmeriCorps management indicated that the assigned GSS and eSPAN stakeholders did not have the opportunity to collaborate on acceptable downtimes and objectives because resource constraints stemming from contract restructuring, staff reductions that removed system owners, and AmeriCorps' realignment have impacted coordination efforts. However, AmeriCorps stated that, with the identification of new system owners, the annual review of the GSS and eSPAN BIAs will now occur to ensure RTOs are aligned and consistent across both systems.

The lack of alignment between the RTOs for the GSS and the eSPAN application hinders timely restoration after a system disruption of mission-critical business functions that rely on eSPAN. This may result in prolonged system outages, leading to lost productivity and operational disruptions.

To assist AmeriCorps with consistently implementing their contingency planning processes, we recommend that AmeriCorps' GSS and eSPAN system owners:

Recommendation 9: Coordinate with relevant stakeholders to align the documented RTOs in the GSS and eSPAN BIAs and ensure both BIAs are updated accordingly.

[19] According to NIST SP 800-34, Revision 1, *Contingency Planning Guide for Federal Information Systems*, "RTO" defines the maximum amount of time that a system resource can remain unavailable before there is an unacceptable impact on other system resources, supported mission/business processes, and the Maximum Tolerable Downtime (MTD). The MTD represents the total amount of time the system owner/authorizing official is willing to accept for a mission/business process outage or disruption and includes all impact considerations.

APPENDIX A: BACKGROUND

AmeriCorps[20] was established in 1993 to provide opportunities for Americans to serve their communities across the country, working directly with national, regional, or local nonprofit and community organizations to meet critical community needs. Its mission is to improve lives, strengthen communities, and foster civic engagement through service and volunteering. In April 2025, AmeriCorps conducted a large-scale RIF in response to the President's Executive Order 14210, *Implementing the President's 'Department of Government Efficiency' Workforce Optimization Initiative*,[21] issued on February 11, 2025. Almost 85 percent of AmeriCorps staff were placed on administrative leave.

AmeriCorps has an inventory of 23 information systems, with 17 designated as internally operated, 5 as contractor systems, and 1 as a federal shared service provider system. Seventeen of these systems are categorized as moderate-security applications, and the remaining six are categorized as low security.[22] AmeriCorps and its contractors share responsibility for managing the information systems, although AmeriCorps retains responsibility for complying with the FISMA and security control implementation requirements.

The Chief Information Officer (CIO) leads the Office of Information Technology (OIT) and is responsible for executing AmeriCorps' overall information technology (IT) program, as well as for allocating resources to protect the agency's mission and business functions against information security threats in a timely and cost-effective manner. The CIO has delegated authority for managing the Cybersecurity Program to the CISO. The CISO carries out the CIO's security and privacy responsibilities and manages the Cybersecurity Program. The CISO's responsibilities include developing an agency-wide Cybersecurity Program; supervising compliance with AmeriCorps' cybersecurity and IT policies, standards, and procedures; and ensuring that personnel with significant system security responsibilities are adequately trained.

AmeriCorps defines specific organization-defined IT security policies, procedures, and parameters in its *Cybersecurity Policy and Security Control Standards* document, incorporating NIST SP 800-53, Revision 5, as necessary to ensure a consistent security and privacy posture across AmeriCorps.

FISMA Reporting Requirements

OMB and the Department of Homeland Security (DHS) annually provide federal agencies and IGs with instructions for preparing FISMA reports. On January 15, 2025, OMB issued Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*.[23] This memorandum provides reporting guidance for FY 2025 in accordance with FISMA. Each year, IGs are required to complete the IG FISMA Reporting Metrics to assess the effectiveness of their agency's information security program and practices.

[20] Effective October 15, 2020, the operating name of the agency was changed from Corporation for National and Community Service to AmeriCorps.
[21] Executive Order 14210 directed a transformation of the federal government, to include plans for RIFs across federal agencies and requiring consultation with a Department of Government Efficiency team.
[22] 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.
[23] See OMB Memorandum M-25-04 online here.

OMB, the Council of the Inspectors General on Integrity and Efficiency, and other stakeholders collaborated to develop the FY 2025 IG FISMA Reporting Metrics.[24]

One of the goals of the annual FISMA evaluation is to assess agencies' progress toward achieving objectives that strengthen federal cybersecurity. The FY 2025 IG FISMA Reporting Metrics were updated to reflect recent developments, as follows:

- NIST published CSF 2.0 in February 2024, highlighting the critical role that governance plays in managing cybersecurity risks and incorporating cybersecurity into an organization's strategy. The FY 2025 IG FISMA Reporting Metrics therefore added a new IG FISMA function *(*Govern*)* that includes a new domain (Cybersecurity Governance*),* to align with NIST CSF 2.0.
- To align with NIST CSF 2.0, the Cybersecurity Supply Chain Risk Management domain moved from the Identify function to the Govern function, to better reflect agency oversight of supply chain risk.
- The FY 2025 IG FISMA Reporting Metrics introduced a new domain, Risk and Asset Management, in the Identify function to group metrics on system inventory and hardware, software, and data management.
- Five supplemental metrics are in scope for the FY 2025 IG FISMA evaluation, including two new supplemental metrics that are focused on system-level risk management practices critical to achieving Zero Trust Architecture objectives.
- The FY 2025 IG FISMA Reporting Metrics revised the core metric on information system-level risk management to focus on the maturity of agencies' implementation of the NIST Risk Management Framework.

[24] See the FY 2025 IG FISMA Reporting Metrics online here.

SIKICH®

APPENDIX B: OBJECTIVE, SCOPE, AND METHODOLOGY

Objective

The objective of this audit was to assess the effectiveness of AmeriCorps' information security program and practices in accordance with FISMA.

Scope

The scope of this audit covered AmeriCorps' information security program and practices consistent with FISMA and reporting instructions that OMB and DHS issued for FY 2025. The scope also included assessing select controls from NIST SP 800-53, Revision 5, supporting the FY 2025 IG FISMA Reporting Metrics, for a sample of 4 of the 23 information systems in AmeriCorps' system inventory as of March 17, 2025 (**Table 5**).

Table 5: Description of Systems Selected for Testing

System Name	Description
GSS (internally operated)	The GSS provides general automated data processing and support for AmeriCorps and the general public using AmeriCorps IT resources. The GSS hosts or provides connectivity for major applications and supports minor applications, such as office automation, human relations, travel, inventory control system, and Freedom of Information Act (FOIA) and Privacy Act requests.
eSPAN (internally operated)	eSPAN, which includes the eGrants grants management system, is used to process and transmit information in support of the National Service Trust and other AmeriCorps programs, as well as performing some Members Pay functions that have not been migrated to the My AmeriCorps Staff Portal.
A financial management system (internally operated)	A financial management system is a commercial off-the-shelf enterprise financial management software system supporting data exchange with other Federal systems and providing financial planning capabilities and a means to record the financial transactions.
ARC (federal shared service provider)	ARC, part of the U.S. Department of Treasury's Bureau of the Fiscal Service, provides a variety of administrative services to various federal agencies. AmeriCorps provides financial transactions requiring payments and posting to ARC via an interconnection with a financial management system.

Source: AmeriCorps System Inventory

In FY 2025, IGs were required to assess 20 core and five supplemental IG FISMA Reporting Metrics across six function areas—Govern, Identify, Protect, Detect, Respond, and Recover—to determine the effectiveness of the agency's information security program and the maturity level of each function area.

The audit also included an evaluation of whether AmeriCorps took corrective actions to address open recommendations from the FY 2019,[25] FY 2021,[26] and FY 2023[27] FISMA evaluations and the FY 2024 FISMA audit.[28]

[25] *Fiscal Year 2019 Federal Information Security Modernization Act Evaluation of the Corporation for National and Community Service* (OIG Report No. 20-03, January 24, 2020).
[26] *Fiscal Year 2021 Federal Information Security Modernization Act Evaluation of AmeriCorps* (Report No. OIG-EV-22-03, December 15, 2021).
[27] *Fiscal Year 2023 Federal Information Security Modernization Act Evaluation of AmeriCorps* (Report No. OIG-EV-23-08, September 29, 2023).
[28] *FY 2024 Federal Information Security Modernization Act (FISMA) Audit* (Report No. OIG-AR-24-03, November 14, 2024).

The audit covered the period from October 1, 2024, through July 31, 2025. We performed audit fieldwork from March through July 2025

Methodology

We conducted this audit in accordance with *Generally Accepted Government Auditing Standards*, issued by the Comptroller General of the United States. 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 that the evidence obtained provides a reasonable basis for our findings and conclusions based on our audit objective.

To accomplish our audit objective, we completed the following procedures:

- Evaluated key components of AmeriCorps' information security program and practices, consistent with FISMA and with reporting instructions that OMB and DHS issued for FY 2025.
- Focused our testing activities on assessing the maturity of the 20 core and five supplemental IG FISMA Reporting Metrics.
- Inspected security policies, procedures, and documentation.
- Performed inquiries of AmeriCorps management and staff.
- Considered guidance contained in OMB's Memorandum M-25-04, *Fiscal Year 2025 Guidance on Federal Information Security and Privacy Management Requirements*, when planning and conducting our work.
- Evaluated select security processes and controls at the program level, as well as for a non-statistical sample of four of AmeriCorps' internally operated and third-party information systems from the 23 systems in AmeriCorps' system inventory. We considered AmeriCorps' reliance on third-party systems and the purpose of each of AmeriCorps' information systems, then selected three of AmeriCorps' 17 internally operated systems and one federal shared service provider system, for testing. All four systems selected for testing are designated as moderate-impact systems based on NIST Federal Information Processing Standard Publication (FIPS PUB) 199, *Standards for Security Categorization of Federal Information and Information Systems*.
- Analyzed the sample of four systems selected for testing, including reviewing selected system documentation and other relevant information, as well as testing selected security controls to support the IG FISMA Reporting Metrics.
- Reviewed the status of prior-year FISMA recommendations. See **Appendix C** for the status of the prior-year recommendations.

The *FY 2023-2024 IG FISMA Reporting Metrics* introduced a calculated average scoring model that was continued for the FY 2025 FISMA audit. As part of this approach, IGs must average the ratings for core and supplemental IG FISMA Reporting Metrics independently to determine a domain's maturity level and provide data points for the assessed effectiveness of the program and function. To provide IGs with additional flexibility and encourage evaluations that are based on agencies' risk tolerance and threat models, the IG FISMA Reporting Metrics do not automatically round calculated averages to a particular maturity level. In determining maturity levels and the overall effectiveness of the agency's information security program, OMB strongly encouraged IGs to focus on the results of the core IG FISMA Reporting Metrics, as these tie

directly to administration priorities and other high-risk areas. OMB recommended that IGs use the calculated averages of the supplemental IG FISMA Reporting Metrics as a data point to support their risk-based determination of the overall effectiveness of the program and function.

We used the FY 2025 IG FISMA Reporting Metrics guidance[29] to form our conclusions for each CSF domain and function, as well as the overall agency rating. Specifically, we focused on the calculated average scores of the core IG FISMA Reporting Metrics. Additionally, we considered other data points, such as the calculated average scores of the supplemental IG FISMA Reporting Metrics and progress that AmeriCorps has made in addressing outstanding prior-year recommendations, to form our risk-based conclusion.

Our work did not include assessing the sufficiency of internal controls over AmeriCorps' information security program or other matters not specifically outlined in this report.

[29] The FY 2025 IG FISMA Reporting Metrics provided the agency IG with the discretion to determine the rating for each of the CSF domains and functions and the overall agency rating based on the consideration of agency-specific factors and weaknesses noted during the FISMA audit. Using this approach, IGs may determine that a particular domain, function area, or agency information security program is effective at a calculated maturity level lower than level 4.

SIKICH®

APPENDIX C: STATUS OF PRIOR-YEAR RECOMMENDATIONS

The table below summarizes the status of the open prior-year recommendations from the FY 2019, FY 2021, and FY 2023 FISMA evaluations and the FY 2024 FISMA audit.[30] At the time of testing and IG FISMA Reporting Metric submission, 5 of the 15 prior-year recommendations from the evaluations and audits referenced above remained open.

OIG Report No.	Recommendation	Auditor's Position on Status of Recommendations
OIG-20-03	***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 Our testing identified unpatched software, unsupported software, and improper configuration settings that exposed AmeriCorps' network to critical and high-severity vulnerabilities. See Finding 4.
OIG-20-03	***Recommendation 2:*** Ensure that OIT evaluates if the internet connections at the National Civilian Community Corps Campuses and Regional Offices are sufficient to allow patches to be deployed to all devices within the defined risk-based patch timeline in AmeriCorps policy. If the internet connections are determined to be inadequate, develop and implement a plan to enhance the current internet connections.	Closed We inspected evidence that AmeriCorps has implemented alternatives for increased bandwidth and is conducting scans and remediation of the National Civilian Community Corps (NCCC) Campuses.
OIG-20-03	***Recommendation 6:*** Develop and implement a written process to perform periodic reconciliations between Configuration Management Database (CMDB) and the FasseTrack system.	Open We found that AmeriCorps had documented the process for performing reconciliations between the CMDB inventory and the FasseTrack system in the *AmeriCorps Asset Tracking Procedures* document. However, AmeriCorps did not provide evidence that it performed a reconciliation between the CMDB inventory and the FasseTrack system, as documented in the procedures.
OIG-20-03	***Recommendation 23:*** Physically or mechanically disable the networking capability of the laptop used for member badging at the NCCC Pacific Region Campus.	Closed We inspected evidence that AmeriCorps has removed the device from network connections and configured the device to prevent connection to the internet.
OIG-20-03	***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 We inspected evidence that AmeriCorps has documented a process for disposing of paper files when the files have reached their disposal date, in accordance with records management. However,

[30] See footnotes 25, 26, 27, and 28.

OIG Report No.	Recommendation	Auditor's Position on Status of Recommendations
		AmeriCorps is currently identifying the requirements and guidelines for retention of counselor files.
OIG-EV-22-03	***Recommendation 6:*** Develop, document, and communicate an overall Supply Chain Risk Management (SCRM) strategy, implementation plan, and related policies and procedures to guide and govern supply chain risk management activities. If AmeriCorps intends to limit its IT purchases to GSA vendors, it should so state, and indicate who, if anyone, must approve exceptions.	Closed (Superseded by OIG-AR-24-03 Recommendation 2) We inspected evidence that AmeriCorps documented SCRM policies and certain SCRM procedures; however, we found that AmeriCorps has not documented the following procedures: • Procedures for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide. • Procedures for maintaining configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.
OIG-EV-23-08	***Recommendation 5:*** Complete an authorization package that covers the Administrative Resource Center Financial System.	Closed We inspected evidence that AmeriCorps has completed an authorization package that covers the ARC financial system.
OIG-EV-23-08	***Recommendation 10:*** Upgrade and configure its Security Information and Event Management tool to capture all log requirements in accordance with OMB M-21-31.	Closed We inspected evidence that AmeriCorps has captured all log requirements in accordance with OMB M-21-31.
OIG-EV-23-08	***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.	Closed We inspected evidence that AmeriCorps has completed the minimum requirements in accordance with NIST SP 800-34, Revision 1, in documenting the BIA for the application.
OIG-EV-23-08	***Recommendation 15:*** Develop a Business Impact Analysis for Administrative Resource Center Financial System.	Closed We inspected evidence that AmeriCorps has developed a BIA for the ARC financial system.
OIG-AR-24-03	***Recommendation 1:*** Enforce the requirement for the Tier 2 lead to perform the monthly audit of the inventory report.	Closed We inspected evidence of monthly audit inventory reports and validated that AmeriCorps has enforced the requirement for the Tier 2 lead to perform the monthly audit of the inventory report.
OIG-AR-24-03	***Recommendation 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.)	Open We inspected evidence that AmeriCorps has documented SCRM policies and certain SCRM procedures; however, we found that AmeriCorps has not documented the following procedures: • Procedures for assessing and reviewing the supply chain-related risks associated with suppliers or contractors and the system, system component, or system service they provide. • Procedures for maintaining configuration control over system components awaiting service or repair and serviced or repaired components awaiting return to service.

OIG Report No.	Recommendation	Auditor's Position on Status of Recommendations
OIG-AR-24-03	***Recommendation 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.	Open We noted that the scheduled completion date was August 29, 2025, after our audit fieldwork ended in July.
OIG-AR-24-03	***Recommendation 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.)	Closed We inspected evidence that AmeriCorps has completed an Authorization to Use package that covers the ARC financial system.
OIG-AR-24-03	***Recommendation 5:*** Perform a gap analysis by reconciling all Security Information and Event Management solutions that are capturing logs.	Closed We inspected evidence that AmeriCorps has captured all log requirements in accordance with OMB M-21-31.

SIKICH®

APPENDIX D: MANAGEMENT COMMENTS

AmeriCorps

December 22, 2025

To: Lauren Lesko
Assistant Inspector General for Audits

From: Bilal Razzaq
Chief Information Security Officer

Re: AmeriCorps Management Response to Report Number: OIG-AR-25-03 Federal Information Security Modernization Act (FISMA) Audit

This memorandum addresses the request for comments on the Office of Inspector General (OIG) draft report on the Fiscal Year 2025 Federal Information Security Modernization Act (FISMA) Evaluation of AmeriCorps, issued on December 15, 2025.

AmeriCorps acknowledges and appreciates the vital role of OIG's annual FISMA Evaluation audit in strengthening our cybersecurity program. The implementation of corrective action plans and enhancements informed by the OIG's findings and recommendations has been essential to our continued progress. We place high value on these engagements and remain committed to upholding the integrity and significance of the audit process.

AmeriCorps' leadership concurs with the findings presented by the OIG in the FY 2025 FISMA Draft Audit Report. We appreciate the time, communication, and patience invested in this year's audit, as we experienced unprecedented interruptions and reduction in resources throughout this engagement. The actionable steps and risk-based approach provided by the OIG, particularly in identifying opportunities to enhance our cybersecurity program's effectiveness, are highly valued. AmeriCorps remains committed to addressing cybersecurity risks, diligently working to strengthen the maturity of our enterprise-wide cybersecurity program, and elevating cybersecurity maturity across all Cybersecurity Framework domains. In preparation of the 2025 OIG audit, we were committed to improving our cybersecurity maturity by completing the following:

- Ensuring internet connections at the National Civilian Community Corps Campuses (NCCC) and Regional Offices are sufficient to all patch deployment to all devices within the defined risk-based path timelines.
- Physically or mechanically disabled network capabilities of the laptop used for member badging at the NCCC Pacific Region Campus.

- Developed, documented, and communicated an overall Supply Chain Risk Management (SCRM) strategy, implementation plan, and related policies and procedures to guide and govern supply chain risk management activities.
- Completed an authorization package for the Administrative Resource Center Financial System.
- Implemented Event Logging Level1, Level 2, and Level 3 Security Information and Event Management requirements in accordance with OMB M-21-31.
- Conducted a Business Impact Analysis in accordance with NIST SP 800-34, Revision 1 for the Administrative Resource Center Financial System.
- Enforced and validated the completion and requirement for Tier 2 lead to perform monthly audits of the inventory report.
- Performed a gap analysis by reconciling all Security Information and Event Management solutions capturing logs within AmeriCorps.

AmeriCorps remains enthusiastic about the security program improvements achieved through our partnership with the OIG and looks forward to continuing this collaboration. Together, we will continue strengthening our cybersecurity program.

Sincerely,

BILAL RAZZAQ Digitally signed by BILAL RAZZAQ Date: 2025.12.22 13:13:53 -05'00'

Bilal Razzaq

Chief Information Security Officer

cc: Jennifer Bastress Tahmasebi, Interim Agency Head
Charndrea Leonard, Acting Chief Operating Officer Sandra
Washington, Acting Chief Information Officer Sarah
Mirzakhani, Principal, Sikich, LLC
Jeff Davis, Principal, Sikich, LLC

APPENDIX E: ACRONYM LIST

Acronym	Description
ARC	Administrative Resource Center
BIA	Business Impact Analysis
C.F.R.	Code of Federal Regulations
CIO	Chief Information Officer
CISA	Cybersecurity and Infrastructure Security Agency
CISO	Chief Information Security Officer
CMDB	Configuration Management Database
CSF	Cybersecurity Framework
CVE	Common Vulnerabilities and Exposures
CVSS	Common Vulnerability Scoring System
DHS	Department of Homeland Security
EL	Event Logging
ERM	Enterprise Risk Management
eSPAN	Electronic-System for Programs, Agreements and National Service Participants
FIPS PUB	Federal Information Processing Standard Publication
FISMA	Federal Information Security Modernization Act of 2014
FY	Fiscal Year
GAO	Government Accountability Office
GSS	General Support System
IT	Information technology
ISCP	Information System Contingency Plan
KEVs	Known Exploitable Vulnerabilities
NCCC	National Civilian Community Corps
NIST	National Institute of Standards and Technology
OIG	Office of the Inspector General
OIT	Office of Information Technology
OMB	Office of Management and Budget
RIF	Reduction in Force
RTO	Recovery Time Objective
SCA	Security Control Assessment
SCRM	Supply Chain Risk Management
SIA	Security Impact Analysis
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